OIPE JC98
DEC 14 2004
PATENT & TRADEMARK OFFICE

IJW AF

Docket No.: 4481-031 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of

Inventor(s): David M. ARCHIBALD

U.S. Patent Application No. 09/679,078 : Group Art Unit: 2661

Filed: October 5, 2000 : Examiner: KADING, JOSHUA A

For: CORRELATION OF SIGNALLING MESSAGES

TRANSMITTAL OF APPEAL BRIEF

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

December 14, 2004

Sir:

Submitted herewith in triplicate is Appellant David M. ARCHIBALD Appeal Brief in support of the Notice of Appeal filed October 14, 2004. A credit card form in the amount of $500 is submitted herewith. Please charge any shortages of credit any over-payment to Deposit Account 07-1337.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 07-1337 and please credit any excess fees to such deposit account.

Respectfully submitted,

LOWE HAUPTMAN GILMAN & BERNER, LLP

Allan M. Lowe

Allan M. Lowe
Registration No.: 19,641

USPTO Customer No. 22429
1700 Diagonal Road, Suite 300
Alexandria, Virginia 22314
(703) 684-1111AML/alw
(703) 518-5499 Facsimile

BEST AVAILABLE COPY

OIPE JC98
DEC 14 2004
PATENT & TRADEMARK OFFICE

MAIL STOP APPEAL BRIEF-PATENT
4481-031

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Appeal of	Confirmation No. 7765
David M. ARCHIBALD	Group Art Unit: 2661
Serial No. 09/679,078	Examiner: J. Kading
Filed: October 5, 2000	:
For: CORRELATION OF SIGNALLING MESSAGES	

BRIEF ON APPEAL

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

December 14, 2004

Sir:

Further to the Notice of Appeal filed October 14, 2004, herewith are three copies of Appellant's Brief on Appeal in connection with the above-identified application.

Authorization for payment of the requisite fees is attached.

12/15/2004 CNGUYEN 00000024 09679078
01 FC:1402 500.00 OP

This brief contains the following items under the headings and order set forth below:

I. REAL PARTY IN INTEREST

The real party in interest in this appeal is AGILENT TECHNOLOGIES, INC., Palo Alto, California. Agilent is a spin-off of Hewlett-Packard Company, and its website is Agilent.com. One of the Agilent product lines relates to Operation Support Systems (OSS). In this regard, the attention of the Board is directed to Exhibit 1, a multi-page document obtained from the Agilent website, with the title "Agilent Integrated OSS Assurance," and Exhibit 2, entitled "OSS Network Revenue and Service Management Systems" at URL http://we:home.agilent.com/USeng/nav/-536805380.0/pc.html.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals and/or interferences.

III. STATUS OF CLAIMS

Claims 1-17 are pending. Claims 1-17 are rejected. There are no allowed or canceled claims.

IV. STATUS OF AMENDMENTS

An Amendment after final rejection was submitted, but not entered. Although in an Advisory Action mailed October 19, 2004, the Examiner stated the Amendment raised new issues requiring consideration and/or search, in fact, the Amendment was submitted in an attempt to placate the Examiner. Simultaneously with this Brief, Appellant submits an amendment to cure clerical errors in claims 15 and 17. Appellant presumes the amendment will be entered and the claims on appeal as set forth in the Appendix include these changes.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The invention relates to a method of and apparatus for establishing a correlation between contents of signaling messages having different protocols, but relating to a common bearer data item (page 1, lines 4 and 5). The invention is typically used in connection with monitoring Operation Support Systems (page 7, line 9).

In the specific embodiment of Figures 1 and 2, a public switched telephone network (PSTN) 14 includes signaling link 18 employing a SS7 ISUP mode for signaling messages and a time division multiplex (TDM) transmission or bearer channel 20. As indicated by Exhibit 3 from URL http://www.iec.org/online/tutorials/ss7/, SS7 is an abbreviation for signaling system 7 and is an architecture for performing out-of-band signaling in support of call-establishment billing, routing and information-exchange functions of the PSTN. SS7 clarifies functions to be performed by a signaling system network and is a protocol to enable performance of the network. SS7 is a way to offload PSTN signal and control traffic onto a dedicated packet-switched network separate from the circuit-switched bearer network that carries user voice and data traffic. SS7 is also used to offload PSTN data traffic congestion onto a wireless or wireline digital broadband network. As indicated by Exhibits 4 and 5, respectively from the URLs http://www.iec.org./online/tutorials/ss7/glossary.html and http://www.iec.org/online/tutorials/ss7/topic09.html, the term ISUP refers to an ISDN user part for providing signaling for ISDN and non-ISDN calls between switched elements for basic and supplementary services for call establishment, to provide supervision and release of circuit switch network connections for telecommunications services. ISUP controls circuits used to carry voice or data traffic. In addition, the circuits can be verified and managed using ISUP. The management of the circuit infrastructure can occur both at the individual circuit level and

for groups of the circuits. Services that can be defined using ISUP include switching, voicemail and Internet offloading.

The initial address message (IAM) of the SS7 ISUP on signaling link 18 is supplied to media gateway controller 10 that is coupled with media gateway controller 10a via signaling link 22 (page 4, lines 24-31). Link 22 supplies the initial address message (IAM) that link 18 supplied to media gateway controller 10, in SS7 ISUP mode (page 4, lines 27-29). The time division multiplexed signal on channel 20 is supplied to media gateway 12, which in turn supplies the signal to packet network 16, which is, for example, a network that operates in the asynchronous transfer mode (ATM) or in accordance with Internet protocol (IP) (page 4, lines 24-29; Fig. 2 at reference numeral 16).

Media gateway controller 10 and media gateway 12 are coupled together by link 26 that operates in the media gateway control protocol (MGCP) (page 4, lines 34 and 35). As indicated by URL http://webpedia.com/terms/am/mgcp.html, the media gateway control protocol is a control and signal standard for controlling media gateways that, for example, convert audio signals carried on public telephone switched networks to data packets carried over the Internet or other packet networks. Controller 10 responds to the initial address message (IAM) on link 18 to supply a create connection message (CRCX) that link 26 supplies to media gateway 12 (page 5, lines 2 and 3). The CRCX message defines an endpoint for a packet connection of the time division multiplex (TDM) signal on channel 20, that is supplied by media gateway 12 to the defined endpoint of packet network 16 via link 24 (page 5, lines 2 and 3). Packet network 16 supplies media gateway 12 with a signal (via link 24) indicating that the connection has been established for the signal on channel 20 to the defined endpoint in the packet network (page 5, line 4). Media gateway 12 responds to the create connection message CRCX on link 26, and to a successful connection of the time division multiplex signal on channel 20 to the endpoint of packet

network 16 by supplying media gateway controller 10 with a signal OK that is transmitted by the media gateway to media gateway controller 10 via link 26 (page 5, lines 4-6).

Monitoring system 28 is coupled to link 18, while monitoring system 30 is coupled to links 22, 24, and 26 (page 5, lines 34 and 35; reference numerals 28 and 30, Fig. 2). Monitoring systems 28 and 30 were commercially available passive monitoring devices known, at the time the application was prepared, as "hpacceSS7," now known by the trademark acceSS7 and available from Agilent Technologies (page 5, lines 35 and 36). Monitoring systems 28 and 30 detect and generate copies of all signaling messages, including the sequence of signaling messages that set off a call across the network of Figure 1 (page 6, lines 1-6). Hence, monitoring system 28 detects and generates copies of all signaling messages coupled to and from media gateway controller 10 on link 18, while monitoring system 30 detects and generates copies of the messages on link 22, including the initial address messages coupled by media gateway controller 10 to media controller 10a, the create connection CRCX messages and the OK messages on link 26 and the end point assignment and return messages on link 24, between media gateway 12 and packet network 16 (Fig. 2).

The detected and generated copies of the messages monitored by monitoring systems 28 and 30 are coupled to monitoring control center 32 (page 6, lines 3 and 4). Monitoring control center 32 includes processing equipment for analyzing the collected data (page 6, lines 4-6). In addition, monitoring control center 32 performs correlations with regard to between the identifiers of the messages on links 18, 22, 24 and 26, even though these links are operated in accordance with different modes (page 6, lines 4-16). In other words, monitoring control center 32 determines that the identification of the channels carrying the time division multiplex signal on channel 20 is the same as the identification of the channel between media gateway 12 and packet network 16.

VI. GROUND OF REJECTIONS TO BE REVIEWED ON APPEAL

A. The specification is not adequate to enable one of ordinary skill in the art to make and use the invention defined by claims 1-17.

B. One of ordinary skill in the art would not understand the meaning of the term "correlate," as employed in the claims and specification of the present application means.

C. The purpose of a claim is to explain how a method step or apparatus limitation performs a stated result.

VII. ARGUMENTS

Because of the specialized nature of the technology, Appellant includes with this Brief, additional materials concerned with the technology, namely:

Exhibit 6: URL http://www.iec.org/online/tutorials/ss7/topic01.html

Exhibit 7: URL http://www. iec.org/online/tutorials/ss7/topic02.html

Exhibit 8: URL http://www.iec.org/online/tutorials/ss7/topic03.html

Exhibit 9: URL http://www.iec.org/online/tutorials/ss7/topic04.html

Exhibit 10: URL http://www.iec.org/online/tutorials/ss7/topic05.html

Exhibit 11: URL http://www. iec.org/online/tutorials/ss7/topic06.html

Exhibit 12: URL http://www.iec.org/online/tutorials/ss7/topic07.html

Exhibit 13: URL http://www.iec.org/online/tutorials/ss7/topic08.html

Exhibit 14: URL http://www. iec.org/online/tutorials/ss7/topic10.html

Exhibit 15: URL http://www.iec.org/online/tutorials/ss7/topic11.html

Exhibit 16: URL http://www.iec.org/online/tutorials/ss7/topic12.html

The Examiner admitted to attorney for Appellant that he is unfamiliar with the technology. In this regard, see the "Remarks" in the first sentence on page 8 of the Amendment under 37 C.F.R. §1.116 filed September 14, 2004. Given this admission, it is difficult to understand how the Examiner is qualified to determine what is enabling to one of ordinary skill in the art.

A. The Disclosure is Enabling

In rejecting claims 1 and 12, upon which claims 4-6 depend, the Examiner states that the independent claims do not comply with the enablement requirement of 35 U.S.C. §112, first paragraph, because the claims do not indicate how the third messages are used to correlate the first and second bearer channel identifications. The Examiner asks where the third messages come from and states that claims 1 and 12 must explain how a correlation between the content of a signaling message is established.

In response to the questions regarding how the third messages are used to correlate the first and second bearer channel identifications and where the third messages come from, Appellant notes that the purpose of a claim is to define an invention, not to provide an enabling disclosure of the subject matter. The purpose of a claim is to define the invention. "Specifications teach. Claims claim." *SRI International v. Matsushita Electric Corporation of America*, 775 F.2d 1107, 1121, n. 1441 (Fed. Cir. 1985, *en banc*). The enablement requirement of 35 U.S.C. §112, first paragraph, is to describe how to make and use the invention. Hence, the Examiner's statements that claims 1 and 12 must indicate how the third messages are used to correlate the first and second channel bearer identifications and the question as to where the third messages come from are improper questions with regard to the issues of enablement under 35 U.S.C. §112, first paragraph.

In response to the question of how claims 1 and 12 establish a correlation between the contents of signaling messages, Appellant notes that claim 1 indicates that the method of establishing a correlation between the contents of signaling messages is performed by a monitoring step, four selecting steps, and a using step. The apparatus of claim 12, which is used for establishing a correlation between the contents of signaling messages, includes monitoring equipment; first, second, and third selectors; and a correlator.

The steps of claim 1 and the apparatus of claim 12 read on the disclosed embodiment as follows:

The signaling messages that relate to a common bearer data item on bearer channel 20 (FIG. 2) are the initial address messages (IAM) supplied by signaling link 18 to gateway controller 10 and the create connection message CRCX that media gateway controller 10 supplies to media gateway 12. The initial address message IAM on signal link 18 is in the SS7 ISUP protocol, while the create connection message CRCX on message link 26 is in the media gateway control protocol MGCP. Monitoring system 28 monitors the initial address message IAM on signal link 18, which comprises the first signaling channel. Monitoring system 30 monitors the create connection message CRCX that media gateway controller 10 supplies to media gateway 12.

Monitoring system 28 selects the initial address message IAM on signaling message 18 that includes an identification related to an end user of the bearer data item on channel 20. The identification related to the end user is identified as the "calling" and "called" parties. The first message that monitoring system 28 selects also includes an identification of a bearer channel that carries the bearer data item. The bearer channel is the channel of channels 20 that includes an originating point code (OPC), a destination point code (DPC), and a circuit identification code (CIC). The values of OPC, DPC, and CIC identify the public service telephone network (PSTN) trunk associated with a call (page 5, lines 20-23).

Monitoring system 30 monitors the create connection message CRCX on signaling link 26 and the OK message on signaling link 26, which are in the MGCP protocol. Monitoring system 30 selects the create connection messages (the second messages of claim 1). The CRCX message includes a second identification of a bearer channel carrying the bearer data item and a call identifier. The second identification is the end point identification of the channel of the asynchronous transfer mode channel 24 that carries the

bearer data item and a call identifier. Monitoring system 30 responds to the OK message (the third message of claim 1), which includes an ISUP initial address message related to an end user of the data item and a call identifier. The end user is informed of the calling and called party addresses. Monitoring control center 32 uses the OK messages (the third messages of claim 1) to establish a correlation between the first bearer channel 20 and the second bearer channel 24, which carries a particular signaling message. The monitoring control center performs its correlation, i.e., identification of the calling and called parties of bearer channels 20 and 24 for the same call, even though the initial address message on signaling link 18 was in the SS7 protocol, and the OK message on link 26 was in the GMCP protocol.

Dependent claim 4 as filed indicates the first messages of claim 1 are SS7 ISUP initial address messages, and the end user identification includes calling and called party addresses. In addition, claim 4 indicates the bearer channel identification comprises an OPC-DPC-CIC combination, which is described in the specification as the identification of the public service telephone network trunk associated with a call and which indicates the originating point code, the destination point code, and the circuit identification code.

Dependent claim 5 as filed indicates the second messages of claim 1 are MGCP create connection messages. In connection with FIG. 3, the specification indicates that the create connection message CRCX transmitted from media gateway controller 10 to media gateway 12 and which is monitored by system 30 includes an endpoint name that identifies the same public service telephone network trunk associated with the same call. In addition, the create connection message (CRCX) includes an identification transaction. Claim 5 also indicates that the second bearer channel identification of claim 1 includes endpoint identifier parameters, i.e., claim 5 defines the subject matter set forth in item 2, FIG. 3. Dependent claim 6, as filed, indicates the third messages of claim 1 include ISUP

initial address messages and the end users in the selected third messages are identified as the calling and called party addresses.

In the final Office Action, the Examiner criticized claims 2 and 13, implying that these claims must explain how the correlation between the contents of the signaling messages is established. In fact, claims 2 and 13 indicate the correlation is established by monitoring steps or monitoring equipment, by four selecting steps or selectors, and by performing a correlation step or using a correlator.

In discussing claims 2 and 13, the final rejection asks how the third and fourth messages are used to correlate the first and second bearer channel identifications. The Examiner also asks from where the second and third messages originate. To comply with 35 U.S.C. §112, first paragraph, it is not necessary for the claim to tell how the third and fourth messages are used to correlate the first and second bearer channel identifications or for the claims to state from where the second and third messages emanate. However, Appellant will read the limitations of claims 2 and 13 on the application as filed to show how the application as filed supports the language of claims 2 and 13.

The preamble, monitoring step, and first selecting step of claim 2 are identical to the preamble, monitoring step, and first selecting step of claim 1. Consequently, the foregoing comments with regard to these portions of claim 1 are applicable to the corresponding portions of claim 2. The second selecting step of claim 2, as filed, is the same as the second selecting step of claim 1, except that the second selecting step of claim 2 requires the second identification of a bearer channel to carry the bearer data item and a transaction identifier. In claim 1, the second identification of a bearer channel carries the bearer data item and a call identifier instead of a transaction identifier. Hence, the second selecting step of claim 2 is the same as the second selecting step of claim 1, except that claim 2 indicates that the create connection message CRCX that message link 26 carries

from controller 10 to media gateway 12 includes a transaction identifier instead of a call identifier.

The third selecting step of claim 2, as filed, is the same as the third selecting step of claim 1, except that the selected third message includes an identification related to an end user of the data item and packet network address information, instead of including an identification related to an end user of the data item and a call identifier. In other words, monitoring system 30 selects OK messages transmitted from media gateway 12 to controller 10 on link 26; the OK message includes an identification related to an end user of the data item and address information of packet network 16.

Claim 2 includes the requirement of selecting fourth messages, including packet network address information and a transaction identifier. In the specific embodiment, the fourth messages are MGCP response messages as indicated by dependent claim 7 of the application as filed. The packet network address information comprises an SDP connection descriptor parameter as also indicated in claim 7 as filed. The transaction identifier in the selected fourth message of the preferred embodiment includes transaction identifier parameters, also indicated by claim 7 as filed. Thus, in the preferred embodiment, the selected fourth messages are the OK messages transmitted from media gateway 12 to media gateway controller 10 on message link 26. These OK messages include address information in packet network 16 and a parameter that identifies the transaction.

Monitoring control center 32 responds to the third and fourth messages selected by monitoring system 30 to establish a correlation between the bearer channel of PSTN 20 and the bearer channel of the asynchronous transfer mode or Internet protocol channel 24.

Apparatus claim 13 includes the above limitations of claim 2 but in apparatus language, rather than method format.

The final Office Action implies that 35 U.S.C. §112, first paragraph, is not satisfied because claims 8 and 14 do not define steps or apparatus for establishing a correlation between the contents of the signaling messages. Claim 8 includes a monitoring step, two selecting steps, a determining step, and a correlation-establishing step that defines the method of establishing a correlation between the contents of signaling messages conforming to different protocols. Apparatus claim 14 recites two monitors, two selectors, and a correlator of an apparatus for establishing a correlation between the contents of signaling messages. Consequently, claims 8 and 14 do explain how the correlation is established.

The Examiner also asks how the correlator of claim 14 establishes a correlation between first and second messages. In a related question, the Examiner asks how the correlation step of claim 8 establishes a correlation between the first and second messages.

The first and second messages of claims 8 and 14 are, in the disclosed preferred embodiment, the same as the first and second messages of claim 1. Consequently, the above-noted remarks regarding the first and second messages of claim 1 are applicable to claim 8. Monitoring control center 32 responds to outputs of monitoring system 28 and 30, which are respectively in the SS7 and MGCP protocols and are on links 18 and 26, to establish a correlation between messages on channel 20 of public service telephone network and the asynchronous transfer mode (ATM) channels 24 or the Internet protocol (IP) channels.

Claim 10, which depends on claim 8 and was originally filed, indicates the first messages of claim 8 are SS7 ISUP initial address messages, and the first bearer channel

identification comprises an OPC-DPC-CIC combination. The description of FIG. 3 in the specification indicates the OPC-DPC-CIC combination is an identifier of the public switched telephone network (PSTN) trunk associated with a call and indicates the originating point code, destination point code, and circuit identification code.

Dependent claim 11, as filed, indicates the second messages of claim 8 are MGCP create connection messages and the second channel identification comprises endpoint identifier parameters. FIG. 3 and the description thereof indicate the MGCP create connection messages are transmitted from gateway controller 10 to gateway 12 as a create connection message on message link 26.

As indicated by the enclosed Declaration of David Coker, those skilled in the art would, at the time the application was filed, understand that the calling and called address parameters are used to obtain the correlation of the different messages merely by comparing a pair of values. Mr. Coker is a qualified UK and European Patent attorney who is familiar with the skill level of those working in the field at the time the application was filed. He was able to provide the information set forth in paragraphs 4-7 of his Declaration, even though his skill level is no greater and probably less than those of ordinary skill in the art (paragraph 2 of his Declaration).

Mr. Coker testifies that to obtain the correlation, the calling and called address parameters of one initial address message are compared with the calling and called address parameters of another initial address message. The correlation in this case merely involves the concatenation and comparison of the two address parameters. For example, in the case of a phone call, the address parameters are phone numbers. If a first person at phone number 44118974302 were to call a second person at 01703684111, the calling parameter would be 44118974302 and the called parameter would be 01703684111. The initial address messages that would be correlated both have combined parameters of

44189743202-01703684111. The recognition that both initial address messages have the same value of concatenated parameters enables them to be correlated. The fact that the initial address messages have address parameters of this type, i.e., phone numbers in the foregoing example, and the basic action of comparing the values of the calling and called phone numbers to recognize the initial address messages relating to the same call to obtain the correlation was well-known to those of ordinary skill in the art at the time the application was filed.

Mr. Coker also testifies that one of ordinary skill would have known, at the time the application was filed, that monitoring control center 32 correlates the session description protocol (SDP) connection description parameter included in the initial address message on link 22 between media gateway controllers 10 and 10a with the OK message from media gateway 12 to media gateway controller 10 on link 26 by associating the session description protocol (SDP) description parameter in the initial address message in the SS7 mode on message link 18, as monitored by monitoring system 28, and the SDP connection description parameter in the OK message that gateway 12 transmits to media gateway controller 10. The OK message is defined in the MGCP protocol. The SDP connection description typically comprises the combination (concatenation) of a network type, such as IN, an address type, such as IP4, an IP address, such as 123.231.132.213 and a port number such as 32003. Consequently, the initial address message supplied to media gateway controller 10 on link 18 and the OK message supplied by link 26 to controller 10 both have the same value of SDP connection description parameter, for example, IN IP4 123.231.132.213 32003. The format of the SDP connection description parameter is spelled out in the IETF RFC (="standard") 2327 (Session Description Protocol). Because the initial address message supplied to controller 10 on link 18 and the OK message supplied to controller 10 on link 26 both have the same value for the SDP connection

description parameter, correlating the initial address message supplied by link 18 to controller 10 and the OK message supplied to controller 10 on link 26 merely involves making sure both messages have the same value of the SDP connection parameter. Those of ordinary skill in the art at the time the invention was filed were well aware of the use of session description parameters to correlate or associate related messages.

Mr. Coker's Declaration indicates those of ordinary skill would have known, at the time the application was filed, that monitoring control center 32 correlates the OK message from media gateway 12 to media gateway controller 10 on link 26 with the CRCX message from controller 10 to gateway 12 on link 26 by responding to outputs of monitoring system 30 that are responsive to the messages on link 26. To perform this correlation, monitoring control center 32 associates the transaction identification included in the CRCX and OK messages. The transaction identification identifies a transaction and has the same value in two messages that both relate to the same transaction. A transaction identification is simply a number between 0 and 999,999,999. Those of ordinary skill in the art at the time the application was filed were well aware that the correlation of related messages is obtained by determining if the transaction identifications included in the messages are the same.

Mr. Coker's Declaration also states that those of ordinary skill knew, at the time the application was filed, the existence and format of these various parameters are defined in international and/or industry standards. Their existence and use (by comparing values) to recognize a transaction to which the message relates were, at the time the application was filed, well known to those of ordinary skill in the art. These parameters are often included precisely to enable identification of some aspect of a transaction. These operations, in themselves, are so fundamental and commonplace in this art that it is not necessary to define them to those of ordinary skill in the art. Any person of ordinary skill in the art who

was told, at the time the application was filed, that two messages of the type discussed in the application can be correlated by reference to the identified parameter would have understood that such a correlation means determining if the value of that parameter is the same in both messages.

Appellant notes that the European Patent Office (EPO), which examines applications to determine if they have a disclosure enabling to those skilled in the art, granted corresponding European Patent EP 1 093 312. No question with respect to the disclosure was raised by the EPO (Coker Declaration, paragraph 8).

B. Conclusion

Appellant, by reading the independent claims on the specific embodiment of the application as filed, has indicated where the third messages of claims 1 and 12 come from and where the third and fourth messages of claims 2 and 13 come from. Appellant has indicated how the monitoring systems 28 and 30 and monitoring control center 32 use the third messages of claims 1 and 12 to correlate the first and second bearer channel identifications. Appellant has demonstrated how monitoring systems 28 and 30 and monitoring control center 32 use the third and fourth messages of claims 2 and 13 to correlate the first and second bearer channel identifications of claims 2 and 13. Appellant has also indicated how monitoring systems 28 and 30 and monitoring control center 32 establish correlations between the first and second messages of claims 8 and 14. The various steps and devices of independent claims 1, 2, 8, 13, and 14 indicate how the correlations between the contents of the signaling messages are established.

Reversal of the final rejection is in order.

If for any reason this Brief is found to be incomplete, or if at any time it appears that a telephone conference with counsel would help advance prosecution, please telephone the undersigned, Appellant's attorney of record.

To the extent necessary, a petition for an extension of time is hereby made under 37 C.F.R. §1.136. Please credit any overpayment or charge any shortage in fees due in connection with the filing of this paper, including extension fees, to Deposit Account No. 07-1337.

Respectfully submitted,
LOWE HAUPTMAN GILMAN & BERNER, LLP

Allan M. Lowe, Registration No. 19,641

1700 Diagonal Road, Suite 310
Alexandria, VA 22314
(703) 684-1111 (telephone)
(703) 518-5499 (telecopier)
AML:alw:rk

VIII. APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

1. A method of establishing a correlation between the contents of signalling messages conforming to different protocols but relating to a common bearer data item, comprising the steps of:

monitoring messages traversing at least first and second signalling channels which conform to respective first and second signalling protocols;

selecting first messages including an identification related to an end user of said bearer data item and a first identification of a bearer channel carrying said bearer data item;

selecting second messages including a second identification of a bearer channel carrying said bearer data item and a call identifier;

selecting third messages including an identification related to an end user of said data item and a call identifier; and

using said selected third messages to establish a correlation between the first and second bearer channel identifications.

2. A method of establishing a correlation between the contents of signalling messages conforming to different protocols but relating to a common bearer data item, comprising the steps of:

monitoring messages traversing at least first and second signalling channels which conform to respective first and second signalling protocols;

selecting first messages including an identification related to an end user of said bearer data item and a first identification of a bearer channel carrying said bearer data item;

selecting second messages including a second identification of a bearer channel carrying said bearer data item and a transaction identifier;

selecting third messages including an identification related to an end user of said data item and packet network address information;

selecting fourth messages including packet network address information and a transaction identifier; and

using said selected third and fourth messages to establish a correlation between the first and second bearer channel identifications.

3. The method of claim **2**, wherein the fourth messages comprise responses to said second messages.

4. The method of claim **1**, wherein the first messages include SS7 ISUP Initial Address Messages, the end user identification comprises calling and called party addresses, and the first bearer channel identification comprises an OPC-DPC-CIC combination.

5. The method of claim **1**, wherein the second messages include MGCP Create Connection messages and the second bearer channel identification comprises endpoint identifier parameters.

6. The method of claim **1**, wherein the third messages include ISUP Initial Address Messages and the end user identification comprises calling and called party addresses.

7. The method of claim **2**, wherein the fourth messages include MGCP Response messages, the packet network address information comprises an SDP connection descriptor parameter, and the transaction identifiers comprise transaction ID parameters.

8. A method of establishing a correlation between the contents of signalling messages conforming to different protocols but relating to a common bearer data item, comprising the steps of:

monitoring messages traversing at least first and second signalling channels which conform to respective first and second signalling protocols;

selecting from among the monitored messages first call initiation messages including a first identification of a bearer channel carrying said bearer data item;

selecting from the monitored messages second call initiation messages including a second identification of a bearer channel carrying said bearer data item;

determining elapsed time between occurrence of said first and second messages; and

establishing a correlation between first and second messages for which the elapsed time is below a predetermined threshold, and thus between the first and second bearer channel identifications.

9. The method of claim **8**, wherein establishment of a correlation between first and second messages is also dependent upon absence of any similar messages within a predetermined time interval.

10. The method of claim **8**, wherein the first messages include SS7 ISUP Initial Address Messages, the end user identification comprises calling and called party addresses, and the first bearer channel identification comprises an OPC-DPC-CIC combination.

11. The method of claim **8**, wherein the second messages are MGCP Create Connection messages and the second bearer channel identification comprises endpoint identifier parameters.

12. Apparatus for establishing a correlation between the contents of signalling messages conforming to different protocols but relating to a common bearer data item, comprising:

monitoring equipment for monitoring messages traversing at least first and second signalling channels which conform to respective first and second signalling protocols;

a first selector for selecting first messages including an identification related to an end user of said bearer data item and a first identification of a bearer channel carrying said bearer data item;

a second selector for selecting second messages including a second identification of a bearer channel carrying said bearer data item and a call identifier;

a third selector for selecting third messages including an identification related to an end user of said data item and a call identifier; and

a correlator for establishing a correlation between the first and second bearer channel identifications in accordance with said selected third messages.

13. Apparatus for establishing a correlation between the contents of signalling messages conforming to different protocols but relating to a common bearer data item, comprising:

monitoring equipment for monitoring messages traversing at least first and second signalling channels which conform to respective first and second signalling protocols;

a first selector for selecting first messages including an identification related to an end user of said bearer data item and a first identification of a bearer channel carrying said bearer data item;

a second selector for selecting second messages including a second identification of a bearer channel carrying said bearer data item and a transaction identifier;

a third selector for selecting third messages including an identification related to an end user of said data item and packet network address information;

a fourth selector for selecting fourth messages including packet network address information and a transaction identifier; and

a correlator for establishing a correlation between the first and second bearer channel identifications in accordance with said selected third and fourth messages.

14. Apparatus for establishing a correlation between the contents of signalling messages conforming to different protocols but relating to a common bearer data item, comprising:

a monitor for monitoring messages traversing at least first and second signalling channels which conform to respective first and second signalling protocols;

a first selector for selecting first call initiation messages including a first identification of a bearer channel carrying said bearer data item;

a second selector for selecting second call initiation messages containing a second identification of a bearer channel carrying said bearer data item;

a monitor for determining elapsed time between occurrence of said first and second messages; and

a correlator for establishing a correlation between first and second messages for which the elapsed time is below a predetermined threshold, and thus between the first and second bearer channel identifications.

15. The method of claim **2**, wherein the first messages include SS7 ISUP Initial Address Messages, the end user identification comprises calling and called party addresses, and the first bearer channel identification comprises an OPC-DOC-CIC combination.

16. The method of claim **2**, wherein the second messages include MGCP Create Connection Messages and the second bearer channel identification comprises endpoint identifier parameters.

17. The method of claim **2**, wherein the third messages include ISUP Initial Address Messages and the end user identification comprises calling and called party addresses.

IX. Evidence Appendix

Exhibit 1 -	Agilent Integrated OSS Assurance
Exhibit 2 -	OSS Network Revenue and Service Management Systems
Exhibit 3-	Signaling System7 (SS7) Definition and Overview
Exhibit 4-	Signaling System7 – Glossary
Exhibit 5-	Signaling System7 – Topic 9 "Layers of SS7 Protocol"
Exhibit 6-	Signaling System7 – Topic 1 – "What is Signaling?"
Exhibit 7-	Signaling System7 – Topic 2 – "What is Out-of-Band Signaling?"
Exhibit 8-	Signaling System7 – Topic 3 – "Signaling Network Architecture"
Exhibit 9-	Signaling System7 – Topic 4 – "The North America Signaling Architecture"
Exhibit 10-	Signaling System7 – Topic 5 – "Basic Signaling Architecture"
Exhibit 11-	Signaling System7 – Topic 6 –"SS& Link Types"
Exhibit 12-	Signaling System7 – Topic 7 – "Basic Call Setup Example"
Exhibit 13-	Signaling System7 – Topic 8 – "Database Query Example"
Exhibit 14-	Signaling System7 – Topic 10 – "What Goes Over the Signaling Link"
Exhibit 15-	Signaling System7 – Topic 11 – "Addressing in the SS7 Network"
Exhibit 16-	Signaling System7 – Topic 12 – "Signal Unit Structure"

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 07-1337 and please credit any excess fees to such deposit account.

Respectfully submitted,

LOWE HAUPTMAN GILMAN & BERNER, LLP

Allan M. Lowe
Registration No.: 19,641

USPTO Customer No. 22429
1700 Diagonal Road, Suite 300
Alexandria, Virginia 22314
(703) 684-1111AML/alw
(703) 518-5499 Facsimile

Agilent Integrated OSS Assurance

A new-generation OSS solution

Accelerate profitability with proven network and service assurance solutions

The challenge
The must-do list for today's communication service providers gets tougher all the time. Get services to market sooner. Accelerate time-to-revenue. Manage quality of service and customer satisfaction. Manage services from end-to-end. Cut operational expenses. Squeeze more value from existing assets.

Say you're not invincible? That seems to be the expectation for carriers competing in today's new-generation communications markets. The lines are blurring between circuit switched and packet switched networks. Legacy and next-generation wireless and wireline services are converging. There's a new world emerging, a world driven by hybrid IP, broadband networks and value-added services.

You have a new-generation service environment that's emerging around you. But do you have a new-generation OSS solution to manage it? With Agilent, the answer is *yes*.

The vision
Top down and bottom up
The Agilent vision brings together service assurance and service fulfillment into tightly integrated management solutions. The Agilent new-generation OSS breaks new ground in management solutions for hybrid networks. It gives you a view of your network and services that is both top-down and bottom-up. It's end-to-end. It's tightly integrated yet totally modular. These are the keystones of Agilent's new-generation OSS strategy.

With an Agilent new-generation OSS solution, you can begin at the top—at the service level—and drill down to correlate service quality with the underlying infrastructure elements, so you can gain immediate insight into the customer's actual experience. Or you can begin at the bottom—with the underlying infrastructure components—and look upward to see how infrastructure issues affect service quality to determine which customers are affected.

Agilent Technologies

The modular approach helps accelerate the ROI for your technology investments.

Agent's new generation OSS strategy enables your organization to get to market sooner with new revenue-generating services that pull more value from your existing assets.

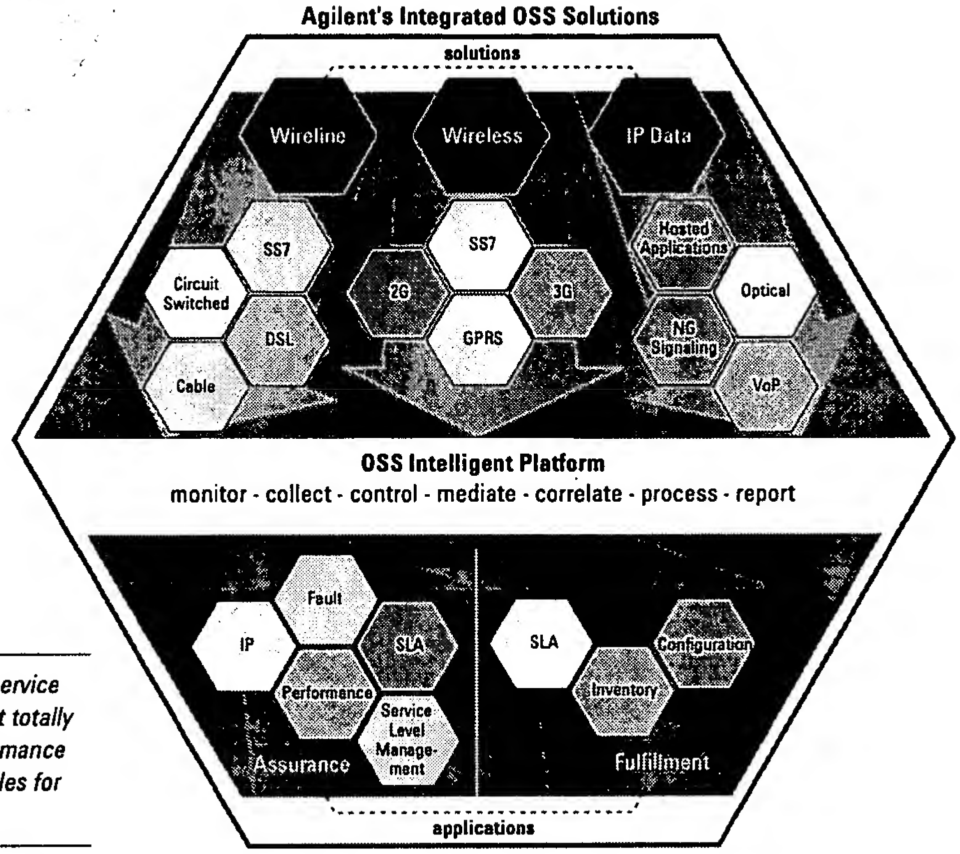
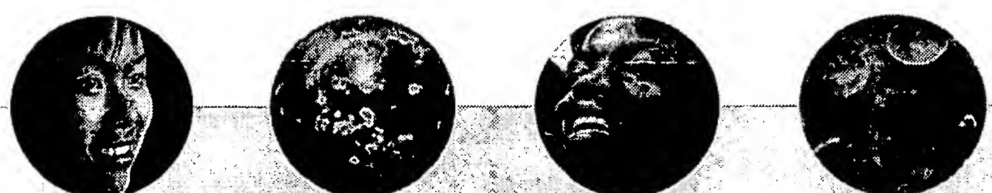


Figure. 1: Agilent Integrated OSS solutions bring together service assurance and service fulfillment into tightly integrated, yet totally modular solutions. Deploy individual service, fault or performance components today to address immediate needs. Add modules for more comprehensive solutions in the future.



The solution

Agilent Integrated OSS Assurance

Agilent Integrated OSS Assurance is the first major integrated solution set to spring from the company's new-generation OSS strategy, consistent with the TeleManagement Forum's NGOSS™ strategy. It brings together Agilent's portfolio of OSS point products into a tightly integrated service assurance solution. It's built on the best-of-class capabilities from Agilent's Firehunter and NETeXPERT product suites. The result is a unified solution for service, fault and performance management.

This is the industry's first fully integrated solution set for end-to-end service assurance in legacy and new-generation wireless and wireline environments. It leverages Agilent's unique combination of measurement and OSS expertise, putting the best of both into an integrated OSS modular solution for service assurance.

*What's this mean to your bottom line? Chances are, your organization is working aggressively to reduce operating expenses and to find new sources of revenue while maintaining customer loyalty. To meet these goals, you need **complete service awareness**. This awareness begins with the ability to correlate, in real time, the actual customer experience with the performance and availability of your service infrastructure, including services components supplied by your partners.*

Only through complete service awareness can you support new value-added service offerings, attract new customers and maintain the consistent, premium service quality levels that keep your customers happy. These are the same goals supported by Agilent Integrated OSS Assurance, a solution set for the new-generation service provider.

To make this strategy achievable and affordable, the Agilent solution integrates and leverages your existing OSS and element-management assets.

A modular approach

Does your organization want to be in the software development business? Probably not. That's not the focus of a communications service provider. To address your OSS assurance needs, you shouldn't have to begin by putting together a team of top-tier software developers.

With the Agilent new-generation OSS strategy, you don't have to be in the software development business. Agilent offers packaged products and modular solutions that allow you to quickly deploy a service assurance solution that is built around pre-integrated, off-the-shelf products.

The modular approach helps accelerate the ROI for your technology investments. It enables your organization to get to market sooner with new revenue-generating services that pull more value from your existing assets.

This modular approach gives you flexibility in your implementation of an integrated OSS assurance solution.

At the same time, the Agilent approach gives you maximum flexibility for today and tomorrow. You can deploy one or more modular solution components now to address immediate and targeted needs. As time goes on, you can add other modules to meet your need for a comprehensive solution that encompasses both service assurance and service fulfillment.

Integrated Service Assurance

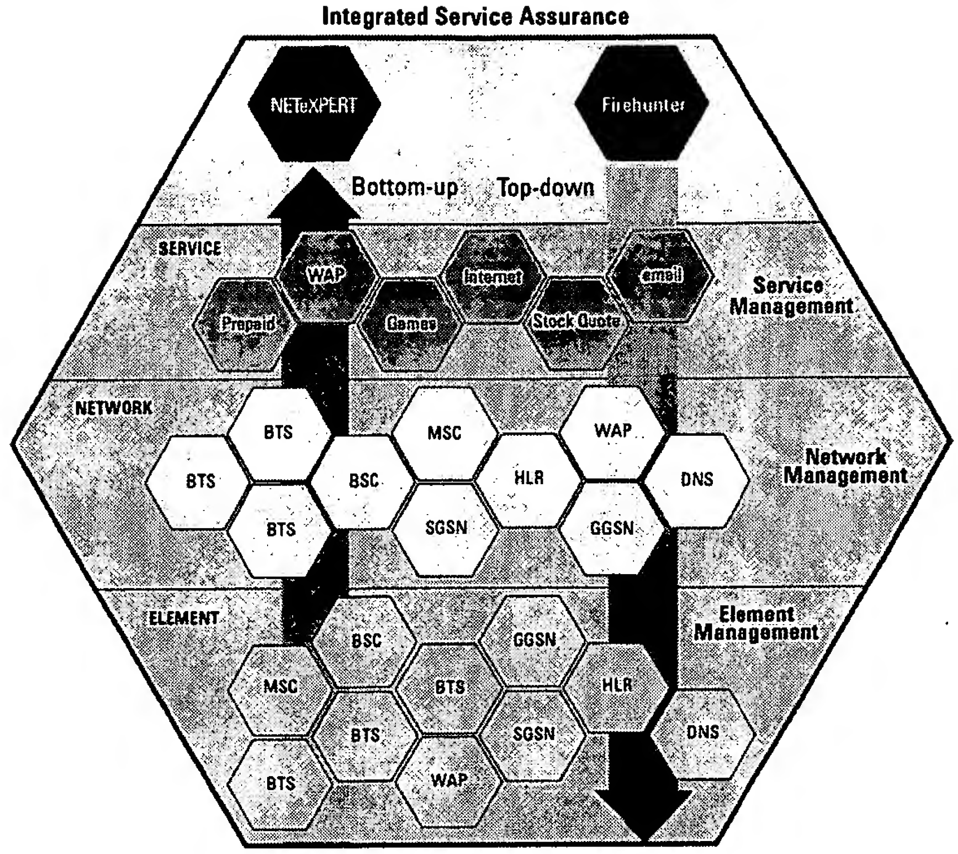


Figure. 2: Tightly integrated solution for service, fault and performance management gives you a view of your network and services that is both top-down and bottom-up. Drill down from the service level to correlate service quality with underlying elements to understand customers' actual experience. Look upward from the underlying components to see how infrastructure issues impact service quality and customers.

Can't do it all at once? With Agilent's new-generation OSS strategy, you don't have to try. You can add value one step at a time.

The components

A modular approach

The Agilent Integrated OSS Assurance solution is made up of tightly integrated modular components. Each component can be deployed as a standalone product that meets targeted needs or can be rolled into a broader, unified solution for OSS assurance. Tying it all together is a state-of-the-art virtual services management (VSM) framework that provides consistent data collection, data management, and data presentation and reporting capabilities.

This modular approach gives you flexibility in your implementation of an integrated OSS assurance solution. You can begin today with one or more modules to meet immediate concerns, and then add modules as your needs grow.

The modular approach is ideal for companies in fast-paced business environments. It makes integration easy, installation quick and configuration straightforward—so you can begin seeing returns on your investment within weeks.

Agilent OSS Service Quality Manager

Agilent OSS Service Quality Manager provides powerful top-down capabilities for managing new-generation IP data services in wireless and wireline environments. Based on the industry-leading Agilent Firehunter solution, Service Quality Manager gathers pertinent data from individual applications, servers, network links and networking equipment to assess end-to-end service performance.

The Agilent Integrated OSS Assurance solution is made up of tightly integrated modular components. Each component can be deployed as a standalone product or can be rolled into a broader, unified solution for OSS assurance.

Service Quality Manager enables you to...

- Automatically discover service elements and build a graphical model of the service environment
- Associate each element with the key tests and measurements needed to verify service availability and performance
- Quickly create service level agreements (SLAs) with pre-defined templates
- Monitor common Internet services and protocols, such as mail, news, Web, DNS, RADIUS and IMAP
- Monitor value-added services and protocols, including those for network performance management, Cisco-equipped networks, Web hosting, VPN, VoIP, WAP and dial-up
- Proactively manage the performance of entire networks, from customer sites through network backbones to customers or applications

Agilent OSS Fault Manager

Based on Agilent's NETeXPERT VSM framework and FM eXEL product, Fault Manager monitors network events to detect and isolate network problems automatically for quick resolution, ensuring high-quality service to customers. Using filters, suppression, thresholding, escalation and correlation, it helps you manage event storms—reducing mean time-to-repair, improving SLA compliance and reducing your costs.

Fault Manager provides bottom-up network surveillance that enables you to...

- Monitor faults and quickly locate network and element outages from a single alarm management console
- Reduce costs by accelerating your ability to build interfaces to new network elements
- Increase customer satisfaction with the ability to administer new policies to manage incoming events
- Increase revenue by turning up services quickly
- Support diverse, multivendor network environments and element management systems

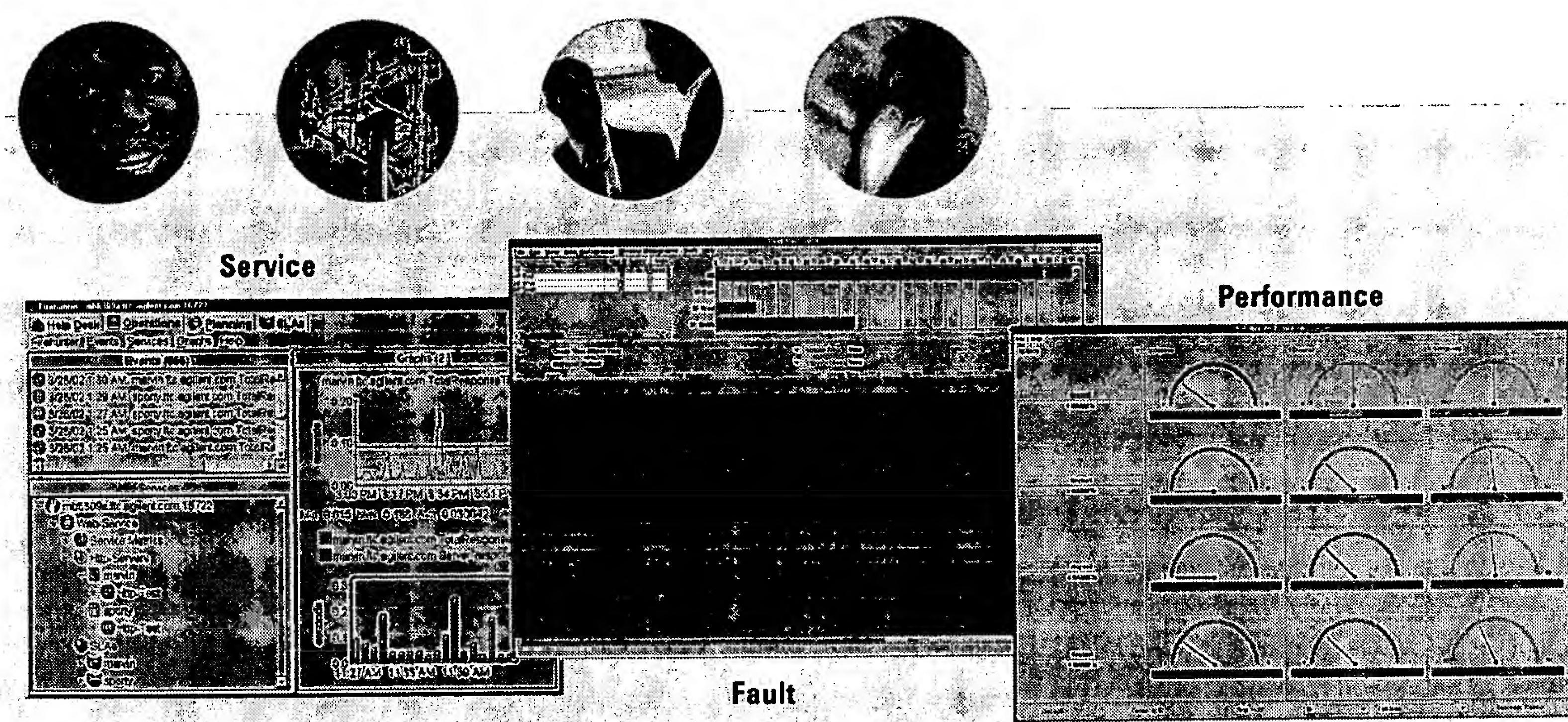


Figure. 3: Only the Agilent solution provides a continuous and complete picture of the service environment with coordinated views of service health, network faults and performance statistics.

Agilent OSS Performance Manager
Agilent OSS Performance Manager, based on NETeXPERT PM eXEL, provides the tools you need to divert performance problems before they affect services. This solution offers advanced performance monitoring and historical reporting to ensure service component availability and operational efficiency. It provides an element-based performance management capability that complements Agilent Service Quality Manager and Fault Manager.

Agilent Performance Manager enables you to...

- Report on performance exceptions as they happen and store data for analysis with live and historical modes
- Proactively monitor networks with views of traffic congestion and long-term performance trends, including graphical wireless reporting (GWR)
- Improve customer satisfaction by assuring service component availability with flexible and customizable reporting tools
- Help control costs through effective network engineering by monitoring both historical and live performance measurements and thresholds
- Ensure high QoS to minimize lost revenue and customer churn by combining element, network and service component impact performance measurements
- Support diverse, multivendor network environments

Agilent OSS Virtual Process Manager
The Agilent Virtual Process Manager provides powerful workflow management capabilities. It delivers solution integration, automation of management processes and control of network and service reconfiguration to recover from faults.

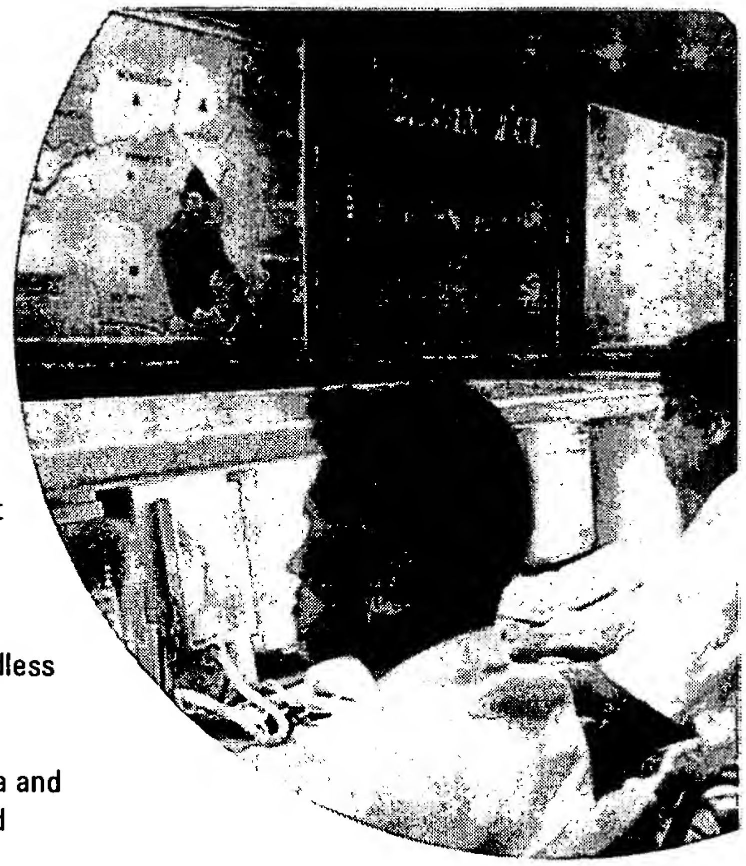
Agilent Virtual Process Manager enables you to...

- Provide automated control and reconfiguration of network and service infrastructure to resolve faults or degraded performance conditions
- Extend your management system easily and cost effectively
- Select and implement network resources regardless of technology or protocol
- Integrate cross-domain applications to share data and processing for end-to-end management solutions
- Create new management applications faster with reusable components, form-based editors and graphical user interfaces
- Support diverse, multivendor network environments
- Incorporate your business processes into your assurance solution to allow you to manage your network in your way
- Track the progress of assurance processes quickly and easily through a Web-based user interface

Agilent IP Assurance Manager
Agilent IP Assurance Manager provides advanced capabilities for IP network service assurance. It continuously monitors network elements and extracts Management Information Base (MIB) data to identify faults and performance problems.

Agilent IP Assurance enables you to...

- Manage systems, hosts, applications and networks efficiently to speed time-to-market
- Maximize infrastructure usage and resolve problems before service is affected, via trending and performance analysis tools, reports and data management for any SNMP device
- Manage duplicate IP addresses to seamlessly manage customer networks that contain IP address collisions
- Increase operational efficiency with distributed autodiscovery of devices beyond corporate firewalls
- Support diverse, multivendor network environments
- Use state-based polling to enable real-time, reactive data collection from elements suspected of contributing to fault and performance problems
- Engage in rapid fault analysis and troubleshooting



Through its ability to integrate data from other systems and tools, the Agilent solution allows you to leverage the best of what you have in place when you deploy your new-generation management solution.

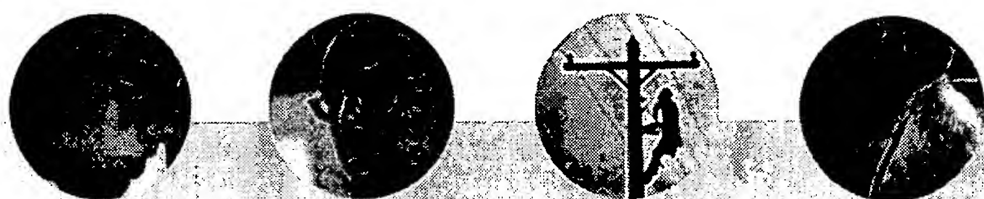
The Agilent approach makes it easy to get your service assurance solution started.

Bringing it all together

Leverage your current investments

Bringing in new technology shouldn't mean throwing out the old. The components of Agilent Integrated OSS Assurance are designed to integrate with your existing element management systems. The solution components can pull data from many point systems and tools, and then incorporate that data into a broader view of your service environment.

Through its ability to integrate data from other systems and tools, the Agilent solution allows you to leverage the best of what you have in place when you



Realize the power of partnerships
Agilent extends its capabilities through partnering with best-in-class technology and service providers, including leading network element providers, independent software vendors, hardware providers and system integrators. Through partners, Agilent provides the element-specific management services and element management system (EMS) integrations that contribute to a complete OSS assurance solution.

This partnering focus makes it possible for Agilent to deliver a stronger, more encompassing service assurance solution that meets more of your needs. Working together with partners, Agilent is able to bring you more comprehensive OSS solutions that fit smoothly into your current management environment.

Be sure with knowledgeable consulting services
Agilent offers expert consulting services to help you tailor your OSS assurance solution to the unique needs of your organization. This can include work to integrate systems, revamp business processes, deploy your solution and support it on an ongoing basis.

Agilent has supplied OSS solutions to hundreds of communication service providers around the world, ranging from wireline and wireless providers to ISPs and ASPs. When you work with Agilent, you leverage the experience gained on countless past projects.

In short, Agilent has what you need to bring it all together quickly—so you can pull the maximum value from your technology investments.

deploy your new-generation management solution. The result is a multi-service, multi-domain solution for wireless, wireline, switched and packet data networks.

What's the big picture? You gain a richer view of your service environment and the insight you need for proactive service-driven management while holding the line on capital expenditures.

Let's get started
The Agilent approach makes it easy to get your service assurance solution started. You can launch your solution with a single, modular component. Over time, you can add other modules to expand the scope of your solution. There are no dead ends, here. The first step puts you on an open road to the future.

Want to put your organization on the route to the new generation in OSS assurance? You can take the first step today by contacting your Agilent sales representative to discuss your needs and Agilent's capabilities. The future begins here.

The need	The Agilent Integrated OSS Assurance solution
Reduce capital expenditures	Top-down and bottom-up monitoring of the service environment enables you to quickly identify faulty assets and over- or under-utilized assets. This information promotes efficient, focused investments that improve services and generate growth.
Accelerate ROI	A modular approach based on pre-integrated, off-the-shelf products allows you to quickly deploy solution components that support new service offerings and generate revenue growth, accelerating your returns on your technology investments.
Reduce network operating costs	Best-in-class fault, performance and service management applications provide vital information on network performance, not just volumes of event data. This reduces the requirement for highly skilled operators. It also reduces event numbness and operator burnout.
Improve IT efficiency	A best-in-class framework and pre-integrated applications help you accelerate time-to-market when deploying new services that keep you competitive.
Reduce truck rolls	Bringing together best-in-class network, system and service management capabilities provides complete service awareness. Drill up from network faults to affected services and drill down from affected services to network faults. Preempt problems before they affect customers and reduce unnecessary truck rolls.
Grow your customer base, reduce churn	Service management and SLA automation improves the quality of service—directly reducing churn and improving customer loyalty.
Protect earned revenue	Leverage service management and monitoring capabilities to ensure that your partners meet SLAs and to prevent the need to grant rebates.
Exploit data to improve marketing and planning	Collect and manage network, system and service performance data across wireline, wireless and IP networks. Intelligent OSS applications convert raw data from multiple sources into useful information to support marketing and planning functions.
Streamline workflows to improve efficiency and reduce human error	Capture, control, and automate core processes through robust workflow capabilities. Track and manage troubleshooting, testing and planning processes. Manage jeopardy situations when tasks and processes are not completed in a timely manner. Automate network and service configuration. Track milestones in meeting SLAs. Ensure consistency in customer care processes.

Discover the new-generation OSS solution

www.agilent.com/comms/oss

#1 Service Assurance Supplier Worldwide
RHK OSS report, 2002

NGOSS™ is a trademark of TeleManagementFORUM

For more information about Agilent OSS Solutions, visit our website or call one of the following customer contact centers:

Argentina	+54 11 5811 7115
Australia	1800 629 485
Austria	+43 (01)25 125 7006
Belgium	+32 (0) 2 404 9340
Brazil	+55 11 4197 3600
Canada-English	877 894 4414
Canada-French	877 894 4414
China	800 810 0189
Denmark	+45 70 13 15 15
Finland	+358 (0) 10 855 2100
France	+33 (0) 825 010 700
Germany	+49 (0) 18 05 24 63 33
Hong Kong	800 930 871
India	1600 112-929
Ireland	+353 1890 924 204
Israel	+972 3 6892 500
Italy	+39 02 92 60 8484
Japan	0120 421 345
Luxemborg	+32 (0) 2 404 9340
Malaysia	1800 888 848
Mexico	+52 01800 506 4800
Netherlands	+31 (0) 20 5472111
Norway	+47 23 25 3720
Philippines	1800 1651 0170
Poland	+48 22 723 0066
Russia	+7 095 797 3963
Singapore	1800 375 8100
South Korea	080 769 0800
Spain	+34 91 631 3300
Sweden	0200 88 22 55
Switzerland-German	+41 (0) 1 735 9300
Switzerland-Italian	+39 (0) 2 92 60 8484
Switzerland-French	+33 (0) 825 010 700
Taiwan	0800 047 866
Thailand	1800 226-008
United Kingdom	+44 (0) 7004 666666
USA	800 452 4844

Data Subject to change.

5988-6742EN

Agilent Technologies

OSS Network, Revenue & Service Management Solutions

Select a Country or Area
Contact Us

For purchase and selection assistance:
How to Buy • Request a Quote

Accelerate profitability with proven OSS network, service and revenue assurance solutions

The Agilent Operational Support System (**OSS**) suite of network assurance, service assurance and revenue assurance solutions enable communications service providers to get new services to market quickly, improve quality of service and reduce cost of operations. Our open, modular family of OSS wireline and wireless solutions supports today's and next generation network architectures, helping to improve levels of performance, reduce fault resolution times and enable new value-added IP services.
To view our library of information for OSS Solutions, please register.

If you've already registered, please access the OSS Solutions Library.

The Agilent OSS Commitment

Products & Services

- **OSS Support Services**
  At Agilent, we understand that your OSS is an integral part of your business. Your success depends upon keeping your Agilent OSS up and running at peak performance.
- **OSS Professional Services**
  Agilent offers a full range of professional services to assist you through the communications challenges of today - and tomorrow.
- **OSS Education & Training Services**
  Agilent's OSS Education and Training Program provides you access to the best in class communications test expertise worldwide. View all our available courses.
- **acceSS7 Location**
  Deploy GSM andd GPRS location-based services with city block accuracy regardless of network or handset, with no impact on network operation or performance.
- **QoS Manager (Firehunter)**
  Service quality and performance managment in real-time for wireless, wireline, switched and packet data networks with Agilent OSS QoS Manager (Firehunter).
- **NgN Analysis System**
  Agilent NgN Analysis System is a distributed, remote-controllable network monitoring system for next-generation telephony networks.
- **J7639E OSS Wireless Service Manager**
  Wireless Service Manger provides wireless service providers with the ability to manage the quality of their services from the customers perspective.
- **Wireless QoS Manager**
  Proactive service quality management and end-to-end troubleshooting of mobile voice and data services using active call testing of network and service accessibility, performance and service success rates.

Product Finder
Go

More Details
- Technical Support
- Library
- Education & Training
- Events
- Alliances & Channel Partners

Other Links
- Email Updates

Highlights

Featured Solutions
Latest Updates

Agilent OSS.Solutions
Information for Network and Service Operations Engineers, Managers, and Executives

Customer-Centric Service Manager Press Release
Agilent Technologies Announces Wireless Telecom Industry's First Real-time Customer-Centric Service Managment Solution

3G UMTS Press Release
Agilent Technologies Announces First Active-Call Test System to Manage Performance of Advance 3G Services Based on UMTS Technology

- **Wireless QoS Manager - 3G UMTS**
  Provides an active call test system as well as the capability to validate the quality of service as it traverses end-to-end through 2G, 2.5G, IP and 3G wireless voice and data networks - all from a customer's perspective.
- **Agilent OSS Global Roaming Test Service**
  An automated service to test the service availability and performance of a Wireless Service Providers subscribers when they roam to other networks.
- **Agilent OSS Customer-Centric Service Manager**
  Real-time monitoring and reporting on actual quality of service delivered to your high-value customers, providing a basis for customer-specific, verifiable SLAs.
- **UMTS Performance Analyzer**
  Provides overall visibility of what is happening in the UMTS network at any point in time in order to identify performance issues and trends, and provide the necessary tools to quickly and easily troubleshoot for early resolution
- **acceSS7**
  The Agilent acceSS7 network monitoring system extracts data from all the SS7 links in a network providing a comprehensive picture about the network, calls and services in real time.
- **NETeXPERT - network management solutions**
  NETeXPERT network management and service assurance solutions offers an integrated view of services and networks that lets you manage operations while focusing on business needs
- **accessFIBER 53000 Series**
  accessFIBER supports planning, design, documentation, maintenance and monitoring of the complete physical layer of fiber optical networks.

Key Library Information

In the Library: Data Sheets, Demonstrations & Catalogs · Application Notes & Technical Papers · Manuals & Guides · Product & Safety Notifications · Software & Firmware Downloads · Newsletters, Articles & Presentations · Frequently-Asked Questions (FAQs)

Product Overview: **Wireless Service Manager Product Brief** Wireless Service Manager Product Brief	2003-11-03		
Product Overview: **Wireless Service Manager Business Scenario** Wireless Service Manager Business Scenario	2003-11-03		
Product Overview: **Wireless Service Quality Management Business Scenario** How Agilent's OSS Solutions help wireless service providers manage QoS for a growing range of service offerings - and reduce customer churn.	2003-06-13	56 KB	
Product Overview: **Agilent OSS Wireless QoS Manager**	2003-06-12		

Related Information

Applications, Technologies & Industries

Newsroom

Additional Information

On-Line Education

Signaling System 7 (SS7)

Definition and Overview

Definition

Signaling System 7 (SS7) is an architecture for performing out-of-band signaling in suppor the call-establishment, billing, routing, and information-exchange functions of the public switched telephone network (PSTN). It identifies functions to be performed by a signaling-system network and a protocol to enable their performance.

This tutorial was authored by Art Doskow, Senior Member of Technical Staff–Signaling and Control Architecture Evolution, Bell Atlantic.

Back Next

DOWNLOAD PDF of this tutorial

TABLE OF CONTENTS:

On-Line Education

WebProForums options
Order IEC Web ProForum Tutorials CD-ROM
Sponsorship Prospectus
· Principal Sponsors
Principal Sponsors:
BROWSE
· All
· New Tutorials
· Broadband Access
· Business and Strategy
· Electronic Design Engineering
· Fixed Wireless
· Mobile Wireless
· Network Components and Design
· Optical Technologies and Networks
· OSS, Network Management, and Testing
· Packet Networking
· Services and Applications
· Switching, Signaling, and Network Intelligence
PROGRAMS
· iForums
· Web ProForums
· Virtual Exhibits
· Product Profiles
· Communications Technologies Program
SEARCH
Search!
MEMBER AREA
Our members enjoy exclusive access to selected white papers and multimedia iForums. Consider these and other benefits of our FREE registration, or register by clicking here.

Already a member? Please click here to log in.

Signaling System 7 (SS7)

Glossary

A links	access links
ACM	address complete message
ANM	answer message
B links	bridge links
BIB	backward indicator bit
BSN	backward sequence number
D links	diagonal links
DPC	destination point code
E link	extended link
F link	fully associated link
FIB	forward indicator bit
FISU	fill in signal unit
FSN	forward sequence number
IAM	initial address message
ISDN	integrated services digital network
ISUP	ISDN user part
kbps	kilobits per second
LSSU	link status signal unit
MF	multifrequency
MSU	message signal unit
MTP	message transfer part

OMAP	operations, maintenance, and administration part
OPC	originating point code
PSTN	public switched telephone network
RBOC	regional Bell operating company
RCL	release complete message
REL	release message
RSP	route set prohibited test message
RSR	restricted test message
SCCP	signaling connection control part
SCP	signal control point
SLS	signaling link selection
SS7	signaling system 7
SSP	signal switching Point
STP	signal transfer point
SU	signal unit
TCAP	transaction capabilities application part
TFA	transfer allowed message
TFP	transfer prohibited message
TFR	transfer restricted message

TABLE OF CONTENTS:

Signaling System 7 (SS7)

9. Layers of the SS7 Protocol

As the call-flow examples show, the SS7 network is an interconnected set of network elements that is used to exchange messages in support of telecommunications functions. The SS7 protocol is designed to both facilitate these functions and to maintain the network over which they are provided. Like most modern protocols, the SS7 protocol is layered.

Physical Layer

This defines the physical and electrical characteristics of the signaling links of the SS7 network. Signaling links utilize DS–0 channels and carry raw signaling data at a rate of 56 kbps or 64 kbps (56 kbps is the more common implementation).

Message Transfer Part—Level 2

The level 2 portion of the message transfer part (MTP Level 2) provides link-layer functionality. It ensures that the two end points of a signaling link can reliably exchange signaling messages. It incorporates such capabilities as error checking, flow control, and sequence checking.

Message Transfer Part—Level 3

The level 3 portion of the message transfer part (MTP Level 3) extends the functionality provided by MTP level 2 to provide network layer functionality. It ensures that messages can be delivered between signaling points across the SS7 network regardless of whether they are directly connected. It includes such capabilities as node addressing, routing, alternate routing, and congestion control.

Collectively, MTP levels 2 and 3 are referred to as the message transfer part (MTP).

Signaling Connection Control Part

The signaling connection control part (SCCP) provides two major functions that are lacking in the MTP. The first of these is the capability to address applications within a signaling point. The MTP can only receive and deliver messages from a node as a whole; it does not deal with software applications within a node.

While MTP network-management messages and basic call-setup messages are addressed to a node as a whole, other messages are used by separate applications (referred to as subsystems) within a node. Examples of subsystems are 800 call processing, calling-card processing, advanced intelligent network (AIN), and custom local-area signaling services (CLASS) services (e.g., repeat dialing and call return). The SCCP allows these subsystems to be addressed explicitly.

Global Title Translation

The second function provided by the SCCP is the ability to perform incremental routing using a capability called global title translation (GTT). GTT frees originating signaling points from the burden of having to know every potential destination to which they might have to route a message. A switch can originate a query, for example, and address it to an STP along with a request for GTT. The receiving STP can then examine a portion of the message, make a determination as to where the message should be routed, and then route it.

For example, calling-card queries (used to verify that a call can be properly billed to a calling card) must be routed to an SCP designated by the company that issued the calling card. Rather than maintaining a nationwide database of where such queries should be routed (based on the calling-card number), switches generate queries addressed to their local STPs, which, using GTT, select the correct destination to which the message should be routed. Note that there is no magic here; STPs must maintain a database that enables them to determine where a query should be routed. GTT effectively centralizes the problem and places it in a node (the STP) that has been designed to perform this function.

In performing GTT, an STP does not need to know the exact final destination of a message. It can, instead, perform intermediate GTT, in which it uses its tables to find another STP further along the route to the destination. That STP, in turn, can perform final GTT, routing the message to its actual destination.

Intermediate GTT minimizes the need for STPs to maintain extensive information about nodes that are far removed from them. GTT also is used at the STP to share load among mated SCPs in both normal and failure scenarios. In these instances, when messages arrive at an STP for final GTT and routing to a database, the STP can select from among available redundant SCPs. It can select an SCP on either a priority basis (referred to as primary backup) or so as to equalize the load across all available SCPs (referred to as load sharing).

ISDN User Part (ISUP)

ISUP user part defines the messages and protocol used in the establishment and tear down of voice and data calls over the public switched network (PSN), and to manage the trunk network on which they rely. Despite its name, ISUP is used for both ISDN and non-ISDN calls. In the North American version of SS7, ISUP messages rely exclusively on MTP to transport messages between concerned nodes.

Transaction Capabilities Application Part (TCAP)

TCAP defines the messages and protocol used to communicate between applications (deployed as subsystems) in nodes. It is used for database services such as calling card, 800, and AIN as well as switch-to-switch services including repeat dialing and call return. Because TCAP messages must be delivered to individual applications within the nodes they address, they use the SCCP for transport.

Operations, Maintenance, and Administration Part (OMAP)

OMAP defines messages and protocol designed to assist administrators of the SS7 network. To date, the most fully developed and deployed of these capabilities are procedures for validating network routing tables and for diagnosing link troubles. OMAP includes messages that use both the MTP and SCCP for routing.

Back Next

DOWNLOAD PDF of this tutorial

TABLE OF CONTENTS:

International Engineering Consortium
Catalyzing progress in the information-industry and university communities

About Us | Conferences & Events | Publications | On-Line Education | Contact

IEC Homepage
Press Releases
History
IEC Fellows
Consortium Programs
Student Programs
University Program
Affiliates
Associations/Forums
Media Sponsors and Partners
ECSDEA Affiliate

Calendar
Speaking Opportunities

Overview
Browse Subjects
Top Bestsellers
New Releases
Guidelines for Publication

Overview
iForums
WebProForum tutorials
Virtual Exhibits
Product Profiles
Communications Technologies Program (CTP)
Sponsorship Prospectus

Contact
Email

On-Line Education

WebProForum options
- Order IEC Web ProForum Tutorials CD-ROM
- Sponsorship Prospectus
- Principal Sponsors

Principal Sponsors:

Agilent Technologies
ALCATEL
Cisco Systems
International Engineering Consortium

BROWSE
- New Tutorials
- Broadband Access
- Business and Strategy
- Electronic Design Engineering
- Fixed Wireless
- Mobile Wireless
- Network Components and Design
- Optical Technologies and Networks
- OSS, Network Management, and Testing
- Packet Networking
- Services and Applications
- Switching, Signaling, and Network Intelligence

PROGRAMS
- iForums
- Web ProForums
- Virtual Exhibits
- Product Profiles
- Communications Technologies Program

SEARCH

Search!

MEMBER AREA

Our members enjoy exclusive access to selected white papers and multimedia iForums. Consider these and other benefits of our FREE registration, or register by clicking here.

Already a member? Please click here to log in.

Signaling System 7 (SS7)

1. What is Signaling?

Signaling refers to the exchange of information between call components required to provide and maintain service.

As users of the PSTN, we exchange signaling with network elements all the time. Examples of signaling between a telephone user and the telephone network include: dialing digits, providing dial tone, accessing a voice mailbox, sending a call-waiting tone, dialing *66 (to retry a busy number), etc.

SS7 is a means by which elements of the telephone network exchange information. Information is conveyed in the form of messages. SS7 messages can convey information such as:

- I'm forwarding to you a call placed from 212-555-1234 to 718-555-5678. Look for it on trunk 067.
- Someone just dialed 800-555-1212. Where do I route the call?
- The called subscriber for the call on trunk 11 is busy. Release the call and play a busy tone.
- The route to XXX is congested. Please don't send any messages to XXX unless they are of priority 2 or higher.
- I'm taking trunk 143 out of service for maintenance.

SS7 is characterized by *high-speed packet data* and *out-of-band signaling*.

Back Next

MORE THAN 165 TUTORIALS ARE NOW AVAILABLE ON CD-ROM FOR PROFESSIONALS ON THE GO

DOWNLOAD PDF of this tutorial

TABLE OF CONTENTS:

On-Line Education

WebProForums options
- Order IEC Web ProForum Tutorials CD-ROM
- Sponsorship Prospectus
- Principal Sponsors

BROWSE
- New Tutorials
- Broadband Access
- Business and Strategy
- DSL
- Electronic Design Engineering
- Fixed Wireless
- Mobile Wireless
- Network Components and Design
- Optical Technologies and Networks
- OSS, Network Management, and Testing
- Packet Networking
- Services and Applications
- Switching, Signaling, and Network Intelligence

PROGRAMS
- iForums
- Web ProForums
- Virtual Exhibits
- Product Profiles
- Communications Technologies Program

SEARCH

Search!

MEMBER AREA

Our members enjoy exclusive access to selected white papers and multimedia iForums. Consider these and other benefits of our FREE registration, or register by clicking here.

Already a member? Please click here to log in.

Signaling System 7 (SS7)

2. What is Out-of-Band Signaling?

Out-of-band signaling is signaling that does not take place over the same path as the conversation.

We are used to thinking of signaling as being in-band. We hear dial tone, dial digits, and hear ringing over the same channel on the same pair of wires. When the call completes, we talk over the same path that was used for the signaling. Traditional telephony used to work in this way as well. The signals to set up a call between one switch and another always took place over the same trunk that would eventually carry the call. Signaling took the form of a series of multifrequency (MF) tones, much like touch tone dialing between switches.

Out-of-band signaling establishes a separate digital channel for the exchange of signaling information. This channel is called a signaling link. Signaling links are used to carry all the necessary signaling messages between nodes. Thus, when a call is placed, the dialed digits, trunk selected, and other pertinent information are sent between switches using their signaling links, rather than the trunks which will ultimately carry the conversation. Today, signaling links carry information at a rate of 56 or 64 kbps. It is interesting to note that while SS7 is used only for signaling between network elements, the ISDN D channel extends the concept of out-of-band signaling to the interface between the subscriber and the switch. With ISDN service, signaling that must be conveyed between the user station and the local switch is carried on a separate digital channel called the D channel. The voice or data which comprise the call is carried on one or more B channels.

Why Out-of-Band Signaling?

Out-of-band signaling has several advantages that make it more desirable than traditional in-band signaling.

- It allows for the transport of more data at higher speeds (56 kbps can carry data much faster than MF outpulsing).
- It allows for signaling at any time in the entire duration of the call, not only at the beginning.
- It enables signaling to network elements to which there is no direct trunk connection.

Back Next

TABLE OF CONTENTS:

DOWNLOAD PDF of this tutorial

International Engineering Consortium
Catalyzing progress in the information-industry and university communities

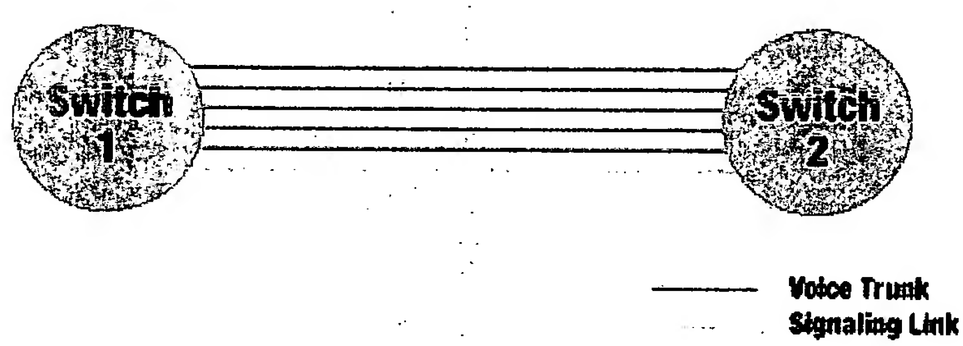
On-Line Education

Signaling System 7 (SS7)

3. Signaling Network Architecture

If signaling is to be carried on a different path from the voice and data traffic it supports, then what should that path look like? The simplest design would be to allocate one of the paths between each interconnected pair of switches as the signaling link. Subject to capacity constraints, all signaling traffic between the two switches could traverse this link. This type of signaling is known as associated signaling, and is shown below in *Figure 1*.

Figure 1. Associated Signaling



Associated signaling works well as long as a switch's only signaling requirements are between itself and other switches to which it has trunks. If call setup and management was the only application of SS7, associated signaling would meet that need simply and efficiently. In fact, much of the out-of-band signaling deployed in Europe today uses associated mode.

The North American implementers of SS7, however, wanted to design a signaling network that would enable any node to exchange signaling with any other SS7-capable node. Clearly, associated signaling becomes much more complicated when it is used to exchange signaling between nodes which do not have a direct connection. From this need, the North American SS7 architecture was born.

Back Next

DOWNLOAD PDF of this tutorial

TABLE OF CONTENTS:

Signaling System 7 (SS7)

4. The North American Signaling Architecture

The North American signaling architecture defines a completely new and separate signaling network. The network is built out of the following three essential components, interconnected by signaling links:

- **signal switching points (SSPs)**—SSPs are telephone switches (end offices or tandems) equipped with SS7-capable software and terminating signaling links. They generally originate, terminate, or switch calls.
- **signal transfer points (STPs)**—STPs are the packet switches of the SS7 network. They receive and route incoming signaling messages towards the proper destination. They also perform specialized routing functions.
- **signal control points (SCPs)**—SCPs are databases that provide information necessary for advanced call-processing capabilities.

Once deployed, the availability of SS7 network is critical to call processing. Unless SSPs can exchange signaling, they cannot complete any interswitch calls. For this reason, the SS7 network is built using a highly redundant architecture. Each individual element also must meet exacting requirements for availability. Finally, protocol has been defined between interconnected elements to facilitate the routing of signaling traffic around any difficulties that may arise in the signaling network.

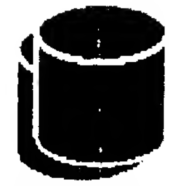
To enable signaling network architectures to be easily communicated and understood, a standard set of symbols was adopted for depicting SS7 networks. Figure 2 shows the symbols that are used to depict these three key elements of any SS7 network.

Figure 2. Signaling Network Elements

STPs and SCPs are customarily deployed in pairs. While elements of a pair are not generally co-located, they work redundantly to perform the same logical function. When drawing complex network diagrams, these pairs may be depicted as a single element for simplicity, as shown in Figure 3.

Figure 3. STP and SCP Pairs

STP Pair



SCP Pair

Back Next

DOWNLOAD PDF of this tutorial

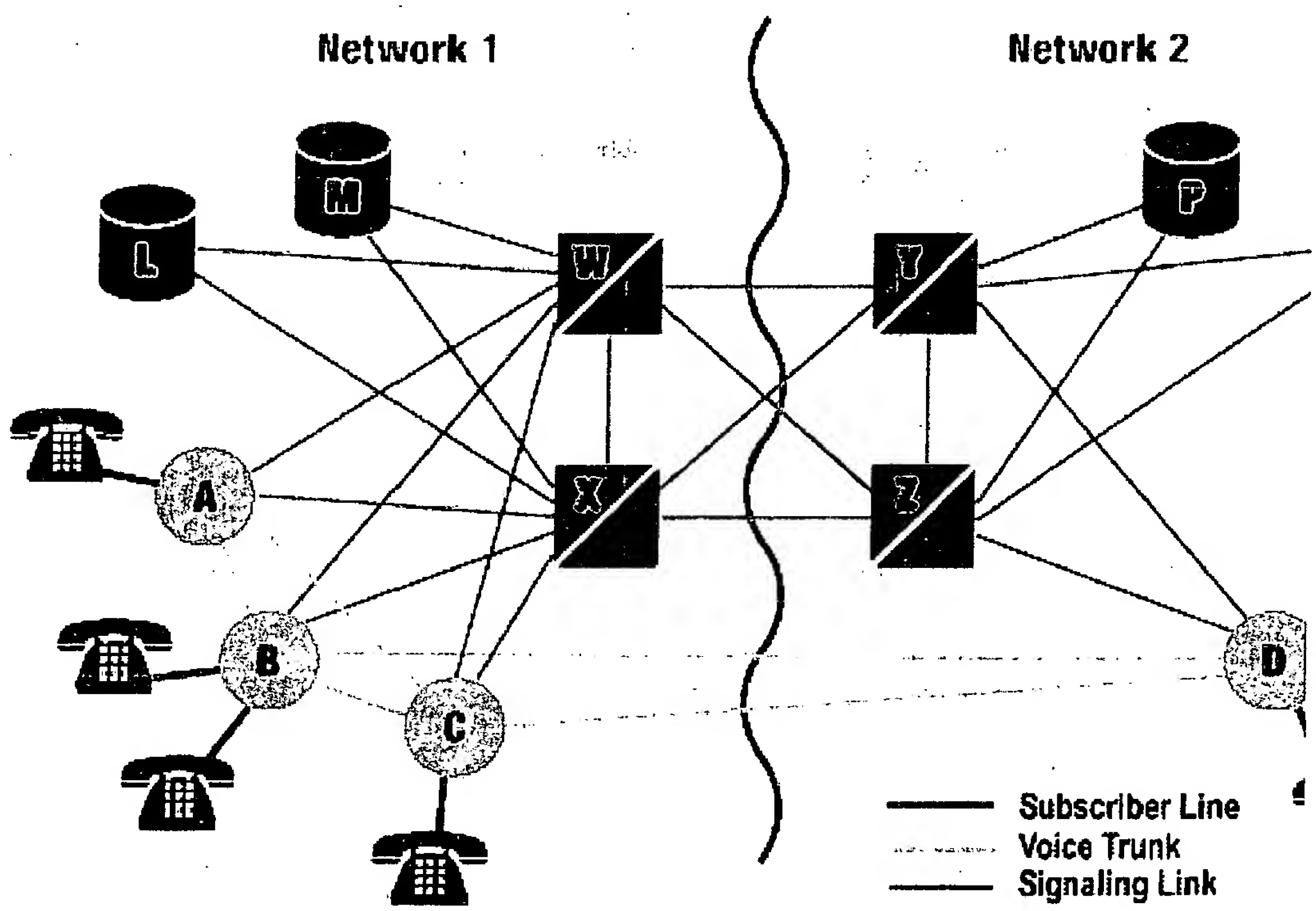
TABLE OF CONTENTS:

Signaling System 7 (SS7)

5. Basic Signaling Architecture

Figure 4 shows a small example of how the basic elements of an SS7 network are deployed to form two interconnected networks.

Figure 4. Sample Network



The following points should be noted:

1. STPs W and X perform identical functions. They are redundant. Together, they are referred to as a mated pair of STPs. Similarly, STPs Y and Z form a mated pair.
2. Each SSP has two links (or sets of links), one to each STP of a mated pair. All SS7 signaling to the rest of the world is sent out over these links. Because the STPs of a mated pair are redundant, messages sent over either link (to either STP) will be treated equivalently.
3. The STPs of a mated pair are joined by a link (or set of links).

4. Two mated pairs of STPs are interconnected by four links (or sets of links). These links are referred to as a quad.
5. SCPs are usually (though not always) deployed in pairs. As with STPs, the SCPs of a pair are intended to function identically. Pairs of SCPs are also referred to as mated pairs of SCPs. Note that they are not directly joined by a pair of links.
6. Signaling architectures such as this, which provide indirect signaling paths between network elements, are referred to as providing quasi-associated signaling.

Back Next

DOWNLOAD PDF of this tutorial

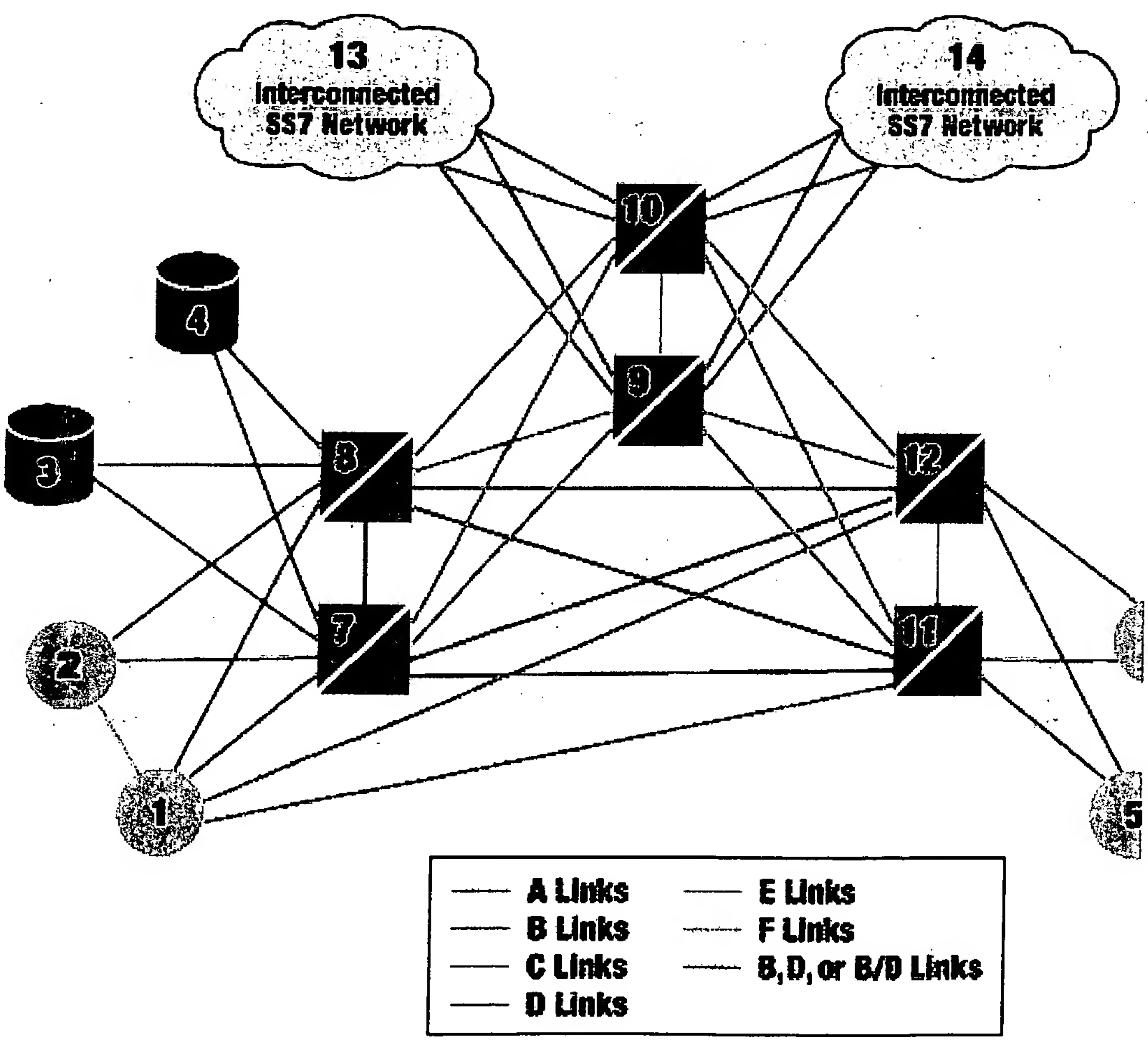
TABLE OF CONTENTS:

Signaling System 7 (SS7)

6. SS7 Link Types

SS7 signaling links are characterized according to their use in the signaling network. Virtually all links are identical in that they are 56-kbps or 64-kbps bidirectional data links that support the same lower layers of the protocol; what is different is their use within a signaling network. The defined link types are shown in *Figure 5* and defined as follows:

Figure 5. Link Types



A Links

A links interconnect an STP and either an SSP or an SCP, which are collectively referred to as signaling end points ("A" stands for access). A links are used for the sole purpose of delivering signaling to or from the signaling end points (they could just as well be referred to as signaling beginning points). Examples of A links are 2-8, 3-7, and 5-12 in Figure 5.

Signaling that an SSP or SCP wishes to send to any other node is sent on either of its A links to its home STP, which, in turn, processes or routes the messages. Similarly, messages intended for an SSP or SCP will be routed to one of its home STPs, which will forward them to the addressed node over its A links.

C Links

C links are links that interconnect mated STPs. As will be seen later, they are used to enhance the reliability of the signaling network in instances where one or several links are unavailable. "C" stands for cross (7-8, 9-10, and 11-12 are C links). B links, D links, and B/D links interconnecting two mated pairs of STPs are referred to as either B links, D links, or B/D links. Regardless of their name, their function is to carry signaling messages beyond their initial point of entry to the signaling network towards their intended destination. The "B" stands for bridge and describes the quad of links interconnecting peer pairs of STPs. The "D" denotes diagonal and describes the quad of links interconnecting mated pairs of STPs at different hierarchical levels. Because there is no clear hierarchy associated with a connection between networks, interconnecting links are referred to as either B, D, or B/D links (7-11 and 7-12 are examples of B links; 8-9 and 7-10 are examples of D links; 10-13 and 9-14 are examples of interconnecting links and can be referred to as B, D, or B/D links).

E Links

While an SSP is connected to its home STP pair by a set of A links, enhanced reliability can be provided by deploying an additional set of links to a second STP pair. These links, called E (extended) links provide backup connectivity to the SS7 network in the event that the home STPs cannot be reached via the A links. While all SS7 networks include A, B/D, and C links, E links may or may not be deployed at the discretion of the network provider. The decision of whether or not to deploy E links can be made by comparing the cost of deployment with the improvement in reliability. (1-11 and 1-12 are E links.)

F Links

F (fully associated) links are links which directly connect two signaling end points. F links allow associated signaling only. Because they bypass the security features provided by an STP, F links are not generally deployed between networks. Their use within an individual network is at the discretion of the network provider. (1-2 is an F link.)

Back Next

DOWNLOAD PDF of this tutorial

TABLE OF CONTENTS:

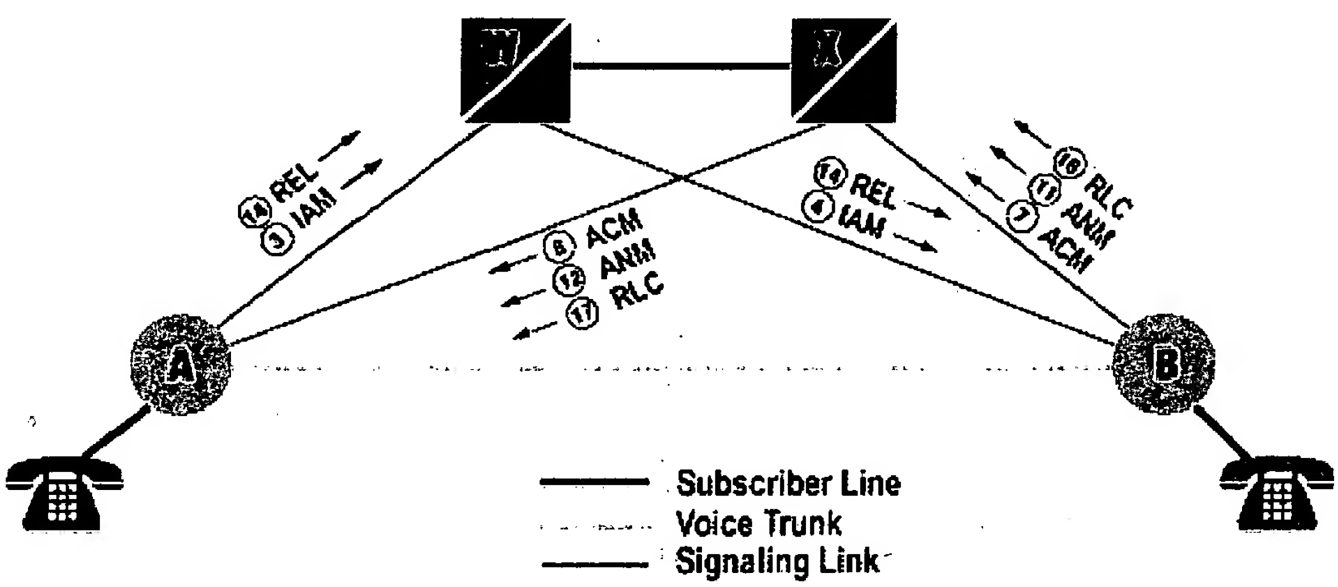
Correct Answers
Glossary
Comment on This Tutorial

Signaling System 7 (SS7)

7. Basic Call Setup Example

Before going into much more detail, it might be helpful to look at several basic calls and the way in which they use SS7 signaling (see *Figure 6*).

Figure 6. Call Setup Example



In this example, a subscriber on switch A places a call to a subscriber on switch B.

1. Switch A analyzes the dialed digits and determines that it needs to send the call to switch B.
2. Switch A selects an idle trunk between itself and switch B and formulates an initial address message (IAM), the basic message necessary to initiate a call. The IAM is addressed to switch B. It identifies the initiating switch (switch A), the destination switch (switch B), the trunk selected, the calling and called numbers, as well as other information beyond the scope of this example.
3. Switch A picks one of its A links (e.g., AW) and transmits the message over the link for routing to switch B.
4. STP W receives a message, inspects its routing label, and determines that it is to be routed to switch B. It transmits the message on link BW.
5. Switch B receives the message. On analyzing the message, it determines that it serves the called number and that the called number is idle.
6. Switch B formulates an address complete message (ACM), which indicates that the IAM has reached its proper destination. The message identifies the recipient switch (A), the sending switch (B), and the selected trunk.
7. Switch B picks one of its A links (e.g., BX) and transmits the ACM over the link for routing to switch A. At the same time, it completes the call path in the backwards direction (towards switch A), sends a ringing tone over that trunk towards switch A, and rings the line of the called subscriber.

8. STP X receives the message, inspects its routing label, and determines that it is to be routed to switch A. It transmits the message on link AX.
9. On receiving the ACM, switch A connects the calling subscriber line to the selected trunk in the backwards direction (so that the caller can hear the ringing sent by switch B).
10. When the called subscriber picks up the phone, switch B formulates an answer message (ANM), identifying the intended recipient switch (A), the sending switch (B), and the selected trunk.
11. Switch B selects the same A link it used to transmit the ACM (link BX) and sends the ANM. By this time, the trunk also must be connected to the called line in both directions (to allow conversation).
12. STP X recognizes that the ANM is addressed to switch A and forwards it over link AX.
13. Switch A ensures that the calling subscriber is connected to the outgoing trunk (in both directions) and that conversation can take place.
14. If the calling subscriber hangs up first (following the conversation), switch A will generate a release message (REL) addressed to switch B, identifying the trunk associated with the call. It sends the message on link AW.
15. STP W receives the REL, determines that it is addressed to switch B, and forwards it using link WB.
16. Switch B receives the REL, disconnects the trunk from the subscriber line, returns the trunk to idle status, generates a release complete message (RLC) addressed back to switch A, and transmits it on link BX. The RLC identifies the trunk used to carry the call.
17. STP X receives the RLC, determines that it is addressed to switch A, and forwards it over link AX.
18. On receiving the RLC, switch A idles the identified trunk.

Back Next

DOWNLOAD PDF of this tutorial

TABLE OF CONTENTS:

On-Line Education

Signaling System 7 (SS7)

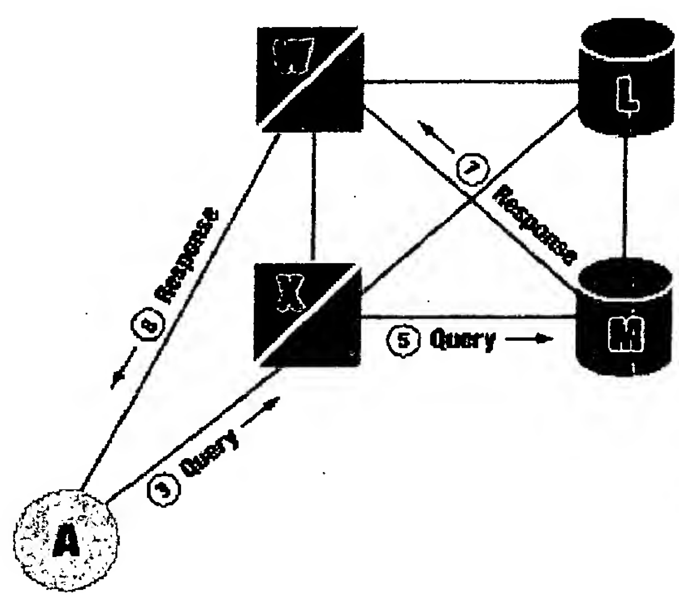
8. Database Query Example

People generally are familiar with the toll-free aspect of 800 (or 888) numbers, but these numbers have significant additional capabilities made possible by the SS7 network. 800 numbers are virtual telephone numbers. Although they are used to point to real telephone numbers, they are not assigned to the subscriber line itself.

When a subscriber dials an 800 number, it is a signal to the switch to suspend the call and seek further instructions from a database. The database will provide either a real phone number to which the call should be directed, or it will identify another network (e.g., a long-distance carrier) to which the call should be routed for further processing. While the response from the database could be the same for every call (as, for example, if you have a personal 800 number), it can be made to vary based on the calling number, the time of day, the day of the week, or a number of other factors.

The following example shows how an 800 call is routed (see *Figure 7*).

Figure 7. Database Query Example



1. A subscriber served by switch A wants to reserve a rental car at a company's nearest location. She dials the company's advertised 800 number.
2. When the subscriber has finished dialing, switch A recognizes that this is an 800 call and that it requires assistance to handle it properly.
3. Switch A formulates an 800 query message including the calling and called number and forwards it to either of its STPs (e.g., X) over its A link to that STP (AX).
4. STP X determines that the received query is an 800 query and selects a database

suitable to respond to the query (e.g., M).

5. STP X forwards the query to SCP M over the appropriate A link (MX). SCP M receives the query, extracts the passed information, and (based on its stored records) selects either a real telephone number or a network (or both) to which the call should be routed.
6. SCP M formulates a response message with the information necessary to properly process the call, addresses it to switch A, picks an STP and an A link to use (e.g., MW), and routes the response.
7. STP W receives the response message, recognizes that it is addressed to switch A, and routes it to A over AW.
8. Switch A receives the response and uses the information to determine where the call should be routed. It then picks a trunk to that destination, generates an IAM, and proceeds (as it did in the previous example) to set up the call.

Back Next

DOWNLOAD PDF of this tutorial

TABLE OF CONTENTS:

About Us | Conferences & Events | Publications | On-Line Education | Contact
IEC Homepage | Calendar | Overview | Overview | Contact
Press Releases | Speaking Opportunities | Browse Subjects | iForums | Email
History | Top Bestsellers | WebProForum tutorials
IEC Fellows | New Releases | Virtual Exhibits
Consortium Programs | Guidelines for Publication | Product Profiles
Student Programs | Communications Technologies Program (CTP)
University Program | Sponsorship Prospectus
Affiliated Associations/Forums
Media Sponsors and Partners
EDSDHA Affiliate

On-Line Education

WebProForum options
Order IEC Web ProForum Tutorials CD-ROM
Sponsorship Prospectus
· Principal Sponsors

BROWSE:
· New Tutorials
· Broadband Access
· Business and Strategy
· Electronic Design Engineering
· Fixed Wireless
· Mobile Wireless
· Network Components and Design
· Optical Technologies and Networks
· OSS, Network Management, and Testing
· Packet Networking
· Services and Applications
· Switching, Signaling, and Network Intelligence

PROGRAMS
· iForums
· Web ProForums
· Virtual Exhibits
· Product Profiles
· Communications Technologies Program

SEARCH

Search

MEMBER AREA

Signaling System 7 (SS7)

10. What Goes Over the Signaling Link

Signaling information is passed over the signaling link in messages, which are called signal units (SUs).

Three types of SUs are defined in the SS7 protocol.

1. message signal units (MSUs)
2. link status signal units (LSSUs)
3. fill-in signal units (FISUs)

SUs are transmitted continuously in both directions on any link that is in service. A signaling point that does not have MSUs or LSSUs to send will send FISUs over the link. The FISUs perform the function suggested by their name; they fill up the signaling link until there is a need to send purposeful signaling. They also facilitate link transmission monitoring and the acknowledgment of other SUs.

All transmission on the signaling link is broken up into 8-bit bytes, referred to as octets. SUs on a link are delimited by a unique 8-bit pattern known as a flag. The flag is defined as the 8-bit pattern "01111110". Because of the possibility that data within an SU would contain this pattern, bit manipulation techniques are used to ensure that the pattern does not occur within the message as it is transmitted over the link. (The SU is reconstructed once it has been taken off the link, and any bit manipulation is reversed.) Thus, any occurrence of the flag on the link indicates the end of one SU and the beginning of another. While in theory two flags could be placed between SUs (one to mark the end of the current message and one to mark the start of the next message), in practice a single flag is used for both purposes.

Back Next

DOWNLOAD PDF of this tutorial

TABLE OF CONTENTS:

Signaling System 7 (SS7)

11. Addressing in the SS7 Network

Every network must have an addressing scheme, and the SS7 network is no different. Network addresses are required so that a node can exchange signaling nodes to which it does not have a physical signaling link. In SS7, addresses are assigned using a three-level hierarchy. Individual signaling points are identified as belonging to a cluster of signaling points. Within that cluster, each signaling point is assigned a member number. Similarly, a cluster is defined as being part of a network. Any node in the American SS7 network can be addressed by a three-level number defined by its network, cluster, and member numbers. Each of these numbers is an 8-bit number and can assume values from 0 to 255. This three-level address is known as the point code of the signaling point. A point code uniquely identifies a signaling point within the American SS7 network and is used whenever it is necessary to address that signaling point.

Network numbers are assigned on a nationwide basis by a neutral party. Regional Bell operating companies (RBOCs), major independent telephone companies, and interexchange carriers (IXCs) already have network numbers assigned. Because network numbers are a relatively scarce resource, companies' networks are expected to meet certain size requirements in order to be assigned a network number. Smaller networks can be assigned one or more cluster numbers within network numbers 1, 2, 3, and 4. The smallest networks are assigned point codes within network number 5. The cluster to which they are assigned is determined by the state in which they are located. The network number 0 is not available for assignment and network number 255 is reserved for future use.

Back Next

DOWNLOAD PDF of this tutorial

TABLE OF CONTENTS:

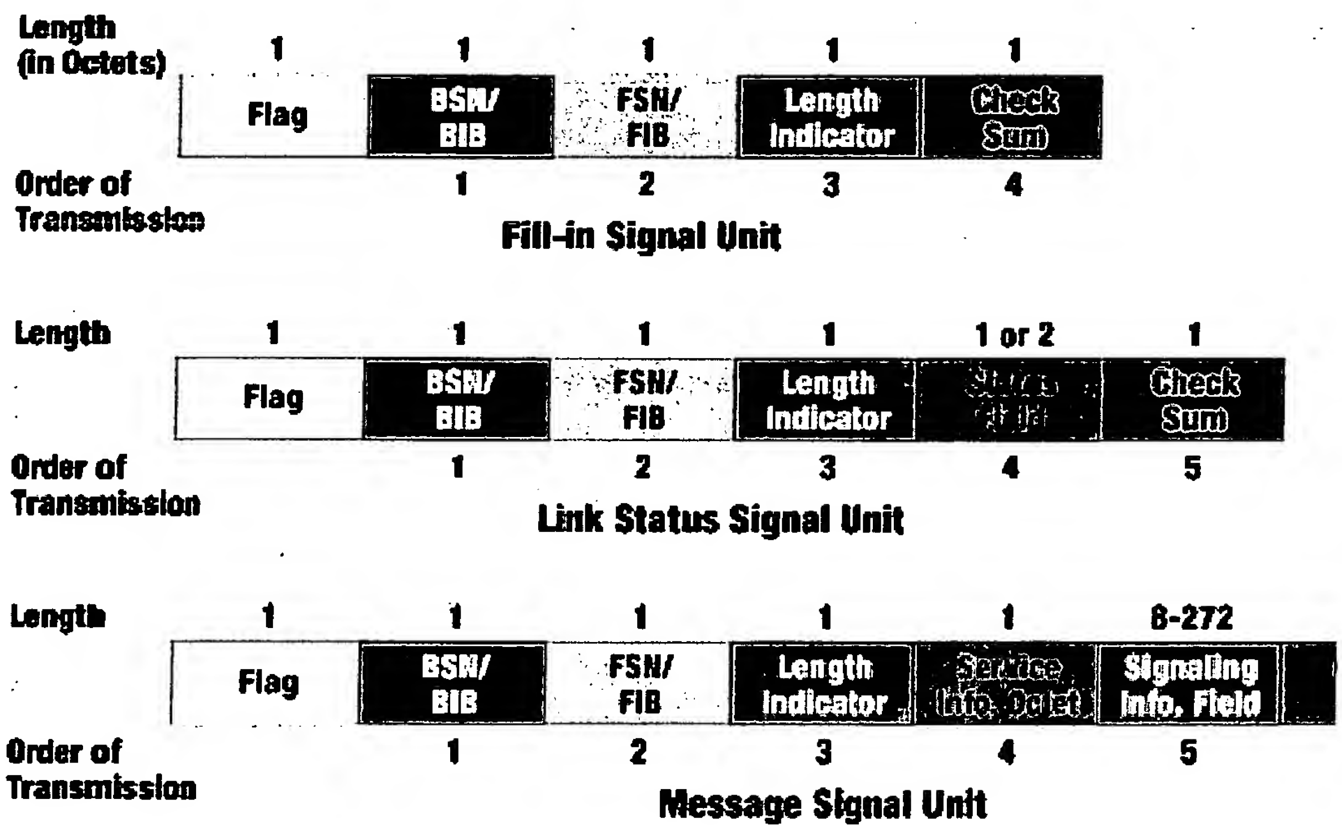
Correct Answers
Glossary
Comment on This Tutorial

Signaling System 7 (SS7)

12. Signal Unit Structure

SUs of each type follow a format unique to that type. A high-level view of those formats is shown in *Figure 8*.

Figure 8. Signaling Unit Formats



All three SU types have a set of common fields that are used by MTP Level 2. They are as follows:

Flag

Flags delimit SUs. A flag marks the end of one SU and the start of the next.

Checksum

The checksum is an 8-bit sum intended to verify that the SU has passed across the link error-free. The checksum is calculated from the transmitted message by the transmitting signaling

point and inserted in the message. On receipt, it is recalculated by the receiving signaling point. If the calculated result differs from the received checksum, the received SU has been corrupted. A retransmission is requested.

Length Indicator

The length indicator indicates the number of octets between itself and the checksum. It serves both as a check on the integrity of the SU and as a means of discriminating between different types of SUs at level 2. As can be inferred from Figure 8, FISUs have a length indicator of 0; LSSUs have a length indicator of 1 or 2 (currently all LSSUs have a length indicator of 1), and MSUs have a length-indicator greater than 2. According to the protocol, only 6 of the 8 bits in the length indicator field are actually used to store this length; thus the largest value that can be accommodated in the length indicator is 63. For MSUs with more than 63 octets following the length indicator, the value of 63 is used.

BSN/BIB FSN/FIB

These octets hold the backwards sequence number (BSN), the backwards indicator bit (BIB), the forward sequence number (FSN), and the forward indicator bit (FIB). These fields are used to confirm receipt of SUs and to ensure that they are received in the order in which they were transmitted. They also are used to provide flow control. MSUs and LSSUs, when transmitted, are assigned a sequence number that is placed in the forward sequence number field of the outgoing SU. This SU is stored by the transmitting signaling point until it is acknowledged by the receiving signaling point.

Because the seven bits allocated to the forward sequence number can store 128 distinct values, it follows that a signaling point is restricted to sending 128 unacknowledged SUs before it must await an acknowledgment. By acknowledging an SU, the receiving node frees that SU's sequence number at the transmitting node, making it available for a new outgoing SU. Signaling points acknowledge receipt of SUs by placing the sequence number of the last correctly received and in-sequence SU in the backwards sequence number of every SU they transmit. In that way, they acknowledge all previously received SUs as well. The forward and backwards indicator bits are used to indicate sequencing or data-corruption errors and to request retransmission.

Back Next

DOWNLOAD PDF of this tutorial

TABLE OF CONTENTS: